NVR5000 Series

User Manual

Release 1.1

About This Document

This manual introduces the hardware components of NVR5000 series and describes how to install them. It also provides an overview of Server surveillance functionality, and includes the functions of Video Management Software for operating and monitoring a Server network.

Version History

Version	Description	Date
1.0	Initial release	December 2014
1.1	VMS 3.1	July 2015

Copyright Statement

Disclaimer

Surveon Technology makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Surveon Technology reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation to notify any person of such revisions or changes. Product specifications are also subject to change without notice.

Trademarks

Surveon and Surveon logo are trademarks of Surveon Technology Inc. Other names prefixed with “NVR” and “SMR” are trademarks of Surveon Technology Inc.

- Microsoft Windows and Windows are registered trademarks of Microsoft Corporation.
- Linux is a trademark of Linux Torvalds.
- Solaris and Java are trademarks of Sun Microsystems, Inc.

All other names, brands, products or services are trademarks or registered trademarks of their respective owners.

Table of Contents

Safety Precautions

Electric Shock Warning

This equipment may cause electric shocks if not handled properly.

- Access to this equipment should only be granted to trained operators and maintenance personnel who have been instructed of, and fully understand the possible hazardous conditions and the consequences of accessing non-field-serviceable units such as the power supplies.
- The system must be unplugged before moving, or in the even that it becomes damaged.

Reliable Grounding

Particular attention should be given to prepare reliable grounding for the power supply connection. It is suggested to use a direct connection to the branch circuit. Check for proper grounding before powering on the device.

Overloading Protection

The device should be installed according to specifications. Provide a suitable power source with electrical overload protection. Do not overload the AC supply branch circuit that provides power to the device.

ESD Precautions

Please observe all conventional anti-ESD methods while handling the device. The use of a grounded wrist strap and an anti-static work pad are recommended. Avoid dust and debris in your work area.

Device Site Recommendations

The device should be installed according to specifications. This device should be operated at a site that is:

- Clean, dry, and free of excessive airborne particles.
- Well-ventilated and away from heat sources such as direct sunlight and radiators.
- Clear of vibration or physical shock.
- Away from strong electromagnetic fields produced by other devices.
- Available with properly grounded wall outlet for power. In regions where power sources are unstable, apply surge suppression.
- Available with sufficient space behind the device for cabling.

Chapter 1. Product Overview

1.1. Features and Benefits

The NVR5316 Linux RAID NVR is part of Surveon Enterprise NVR5000 Series. Featuring 16-bay hot-swappable hard disks and RAID 1, 5, 6 data protection, the NVR5316 supports Full HD (1080P) video recording of up to 64 channels for the video retention period from 7 to 30 days. Based on the client-server architecture, the NVR5316 provides high I/O, large capacities, and overall system stability necessary for scalable projects. The NVR5316 also comes with the enterprise VMS with real-time monitoring and video analytics and supports centralized management and TV wall matrix with the Surveon Control Center (SCC). The compact server NVR size, cableless design, redundant components such as cooling fans and power supplies also ensure excellent system reliability and easy maintenance for middle to large applications.

1.2. Specifications for the NVR5000 Series

1.2.1. Hardware Specifications

	NVR5346 Series
System Processor	NVR5316E1: Intel Core i3 Dual Core 3.5GHz NVR5316A1: Intel Xeon E3 Quad Core 3.2GHz
System Memory	DDR3 4GB (up to 32GB)
Operating System	Linux Embedded System
Storage	16 x 3.5" SATAII/SATAIII hard disk drives
I/O Interface	• RJ-45: 2x Gigabit Ethernet • USB: 2x USB2.0; 2x USB3.0 • VGA: x1, HDMI: x2 • 2x SAS 6G expansion port • 16 pin for 8 in / 2 out
RAID	Non-RAID, RAID 1, 5, 6
Electrical	• Input Voltage: 100-240 VAC, 50~60Hz, 10~5A (max) • Power Supply: two redundant 530W
Operating Environment	Temperature: 5° C to 35° C Humidity: 5% to 80% (non-condensing)
LED Indicator	Yes (Power, HDD, Fan, System Fault)
Dimensions (mm)	130(H) x 448(W) x 500(D) mm
Weight (without hard drives)	21.54kg/47.49lbs (without HDD)
Certificate	UL, CB, FCC/CE Class A
Warranty	3 years

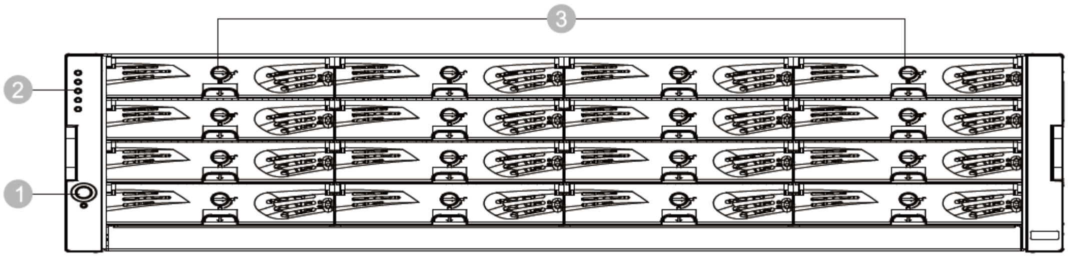
1.2.2. VMS Specifications

Live View	• Real-time network camera discovery • Versatile views of various screen divisions • Multiple views supported • View patrolling for single or multiple views • Real time video/event alarm display • Support 3 installation modes and 5 different fisheye Dewarp display modes • Support live audio
eMAP	• Drag-n-drop camera manipulation •Hierarchical and multiple layer map structure • • Real time event alert • Instant live video of camera
PTZ	• Pan, tilt, zoom operations (depends on camera) • Built-in, floating PTZ control panel • Preset position (dependent of the camera) • Event-driven camera patrolling • Support On-screen PTZ
I/O	• Digital I/O management • Support Ethernet Digital I/O controller
Multiple Displays	• Support dual monitors • Supports live view, playback, eMap functions (depends on product) • Direct display to secondary monitor(s)
Investigation	• Search by date, time and camera • Search by VI event combinations • Search over multiple days • Search over multiple cameras •Different colored recording indicator on calendar • Search via built-in VI analyzer • Intuitive, video thumbnail search results • Cue-in, cue-out and loop playback • Quick playback by video thumbnail • 1/8, 1/4, 1/2, 1x, 2x, 4x, 8x play, pause, stop • AVI-formatted video clip export • Up to 16 channel synchronized playback (depends on product) • Support 3 installation modes and 5 different Fisheye Dewarp playback display modes
Video Intelligence	• General motion detection • Camera motion detection • Missing object detection • Foreign object detection • Intrusion detection • Forbidden area detection • Tampering detection • Virtual Fence • Object Counting (configure on remote client) • Go in/out detection (configure on remote client) • Tailgating detection (configure on remote client)
Recording Policy	• Supports up to 96 channels megapixel recording (depends on product) • Continuous recording • Event-driven recording along with rules • Scheduled recording on daily or weekday basis • Post alarm recording 1-300 seconds • Pre-alarm recording 1-300 seconds • Support individual schedule recording
Rule Manager	• Conditional recording/alert/notification

	• Email, FTP, SMS, popup window, PTZ,VI Panel, Relay output notifications • Sound, alarm, round-the-clock alerts • Support email template
Remote Management	• Remote operation & management via VMS Client • Remote management and control via SCC & SCC Client
Remote Client	• Web Client • iPhone Client • Android Client
3rd Party IPCAM	• Support ONVIF Profile S & ONVIF Scan • ACTi, Arecont Vision, Axis, Dahua, Dynacolor, Hikvision, IQinvision, Mobotix, Panasonic, and more
Storage Expansion	• Built-in RAID storage management • Recording to iSCSI/NAS • Backup to iSCSI/NAS
General & Misc	• Video privacy mask • Digital zoom in, zoom out • Log viewer, log export mechanism • Client auto login • Automatic storage recycling • Client-server architecture • Customized authority account management • Digital watermark proofing • Support DDNS Function • Support time sync with NTP time server • Provide System and VI setup Help assistance • Support Customized Event Management and log mechanism • Auto port mapping for internet connection • Support batch setting IPCAM parameters • Support Health Check function • Support standby recording (Failover) • Support offline recording with Surveon cameras
Language	Support multiple language on VMS including English, Czech, Dutch, French, German, Italian, Japanese, Korean, Persian, Polski, Portuguese, Russian, Slovak, Spanish, Turkish, Simplified Chinese, Traditional Chinese

Chapter 2. Hardware Overview

2.1 Front Panel



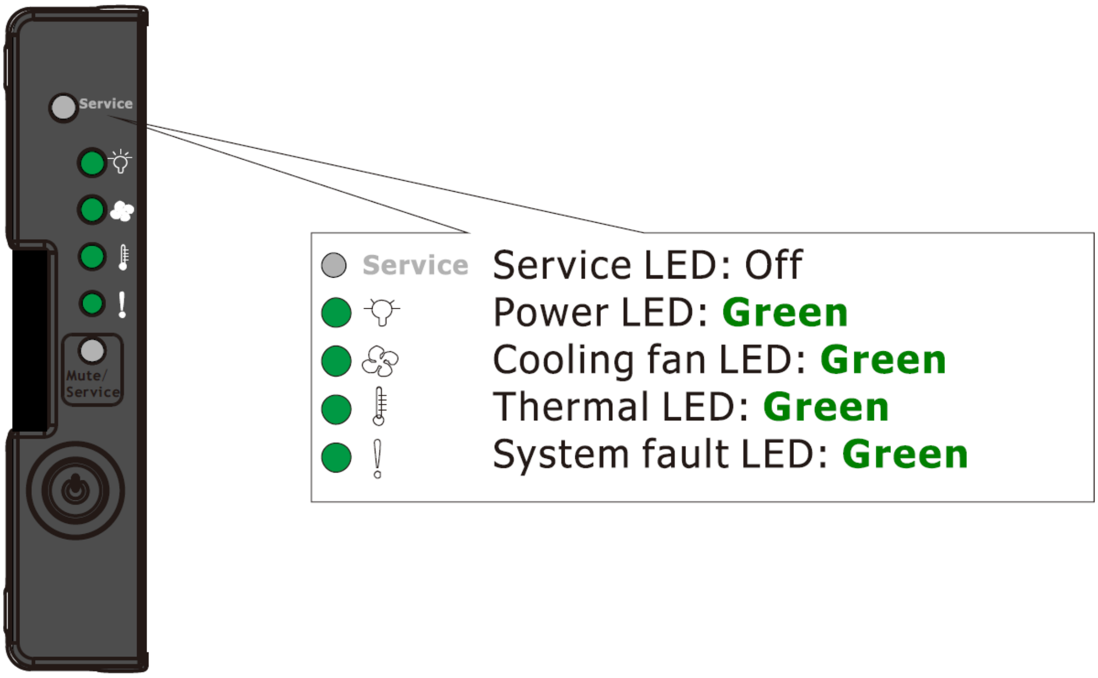
1 Power Button

2 LED Status Indicator

3 HDD Status Indicator

	Function
1. Power Button	Powers up the NVR5000 Series.
2. LED Status Indicator	Indicates the system status.
3. HDD Status Indicator	Indicates the hard disc drive status.

LED Status Indicator



○ Service — Service LED: Off

● Power LED: **Green**

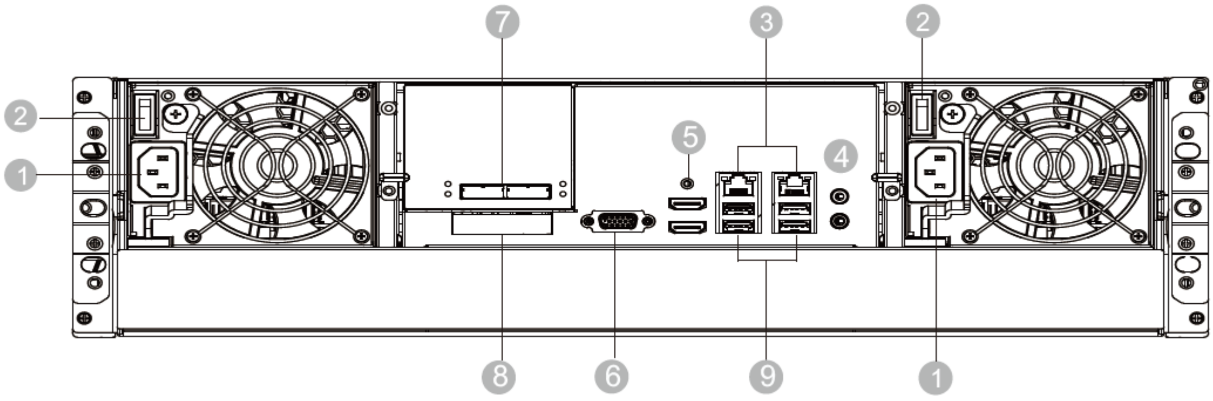
● Cooling fan LED: **Green**

● Thermal LED: **Green**

● System fault LED: **Green**

2.2. Rear Panel

NVR5316 Series



	Function
1. Power Socket	Used for connecting power cable.
2. Power Switch	The power switches are located on the rear panel.
3. LAN Port (GbE Ethernet port)	Used for connecting the NVR5000 Series with the network.
4. Line-Out Mic-In	Used for audio in/out and microphone in.
5. HDMI Port	Used for connecting audio/video devices such as video projectors and DVD players.
6. VGA Port	Used for attaching an external monitor to the NVR5000 Series.
7. SAS Expansion Port	Used for attaching an external SAS JBOD expansion.
8. Digital I/O Port	Used for receiving or sending the singles or data to the system.
9. USB Port x2	Used for exporting video clips as evidence support to external storage devices.

Chapter 3. Software Overview

3.1. Software Introduction

Video Management Software (VMS) is a highly modular and powerful video and hardware management suite that incorporates Server recording, management, and video monitoring and playback functionalities to serve the core purposes of a video surveillance system.

It operates in a client-server mode: The Local Client and Local Domain Server run for standalone SMR/NVR/VMS Server, while the Remote Client receives live video streams and event video playbacks from LAN or Internet. All administrative tasks are performed on the Client. The client software provides the ability to monitoring and playback recorded videos from multiple cameras. And for users having multiple SMR/NVR/VMS Servers, Surveon Control Center (SCC) (its main functions are the same with the VMS) can be utilized to manage over the domain infrastructure.

3.2. Module Framework

- VMS/NVR Server
  - Combines video recording, archival and retrieval functionalities for individual servers/standalone PCs.
  - Serves as the connection point for client stations.
- Local Domain Server
  - The interface between the VMS/VI Servers and any clients.
  - User authentication server.
- Local Client
  - Local access, VMS Client installed on standalone PCs/NVRs for live video monitoring, event recording playback access and VMS system configuration.
- Remote Client (full functions)
  - Remote access, VMS Client installed on remote PCs for live video monitoring, event recording playback access.
  - Serves as the default configuration point for NVR2000 series, which do not have a Local Client.
- Web Client (for simple use)
  - Remote access, an ActiveX application (OCX) installed on remote PCs for live viewing and event playbacks through the web browser.
- SPhone Client (for simple use)
  - SPhone Client installed on iOS/ Android devices for basic live viewing.
- Web Server
  - Allows user to access the live video stream, PTZ control and event recording playbacks through Microsoft Internet Explorer 7.0 (or higher) after the Web Clients components are downloaded.
- VI Server
  - The video intelligence processing point for a VMS solution.
  - Preinstalled on SMR/NVR Server, and optional on a separate server/PC (VMS).
- SCC Domain Server
  - Allows centralized control over multiple Trusted VMS Server points and connections from multiple clients.
- SCC Client

- Software capable of accessing multiple Trusted VMS Servers through the SCC Domain Server

3.3. System Architecture

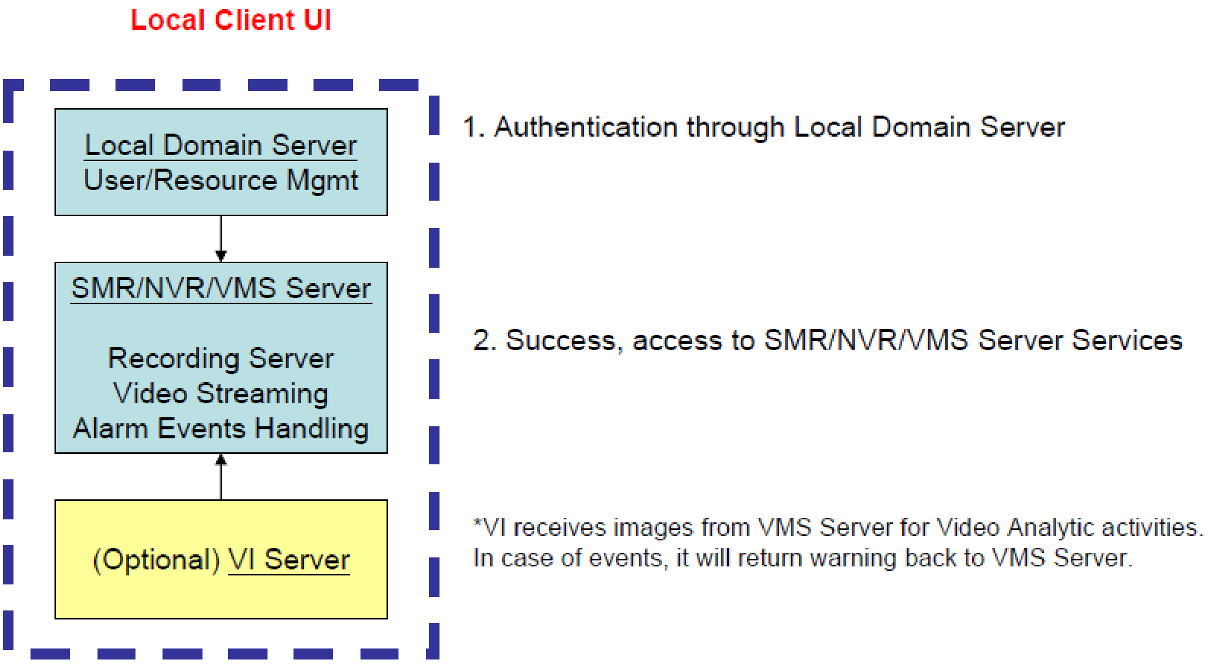
VMS operates in scalable client - server architecture. This architecture can be divided into three types: (1) Standalone Server (2) Standalone Server + Remote Client (Web Client/SPhone Client) (3) Multiple Servers + SCC Client.

These are the hardware requirements for using PCs as Server or Client.

VMS Server + Client			
Support NVRs	≥ 32CH	16~32CH	≤ 16CH
OS	64-bit : Windows 7 Professional, Enterprise, Ultimate		
CPU	Intel Core i7-980X or above	Intel Core i7-860 or above	Intel Core i5-650 or above
Memory	4 GB or above		
Display	nVidia GeForce GTX660 2GB or above		
Hard Drive	SATA 7200 RPM, 500 GB or above		
Network	1 Gbps or above		
Remote Client			
OS	64-bit : Windows 7 Professional, Enterprise, Ultimate		
CPU	Intel Core i7-980X or above	Intel Core i7-860 or above	Intel Core i5-650 or above
Memory	4 GB or above		
Display	nVidia GeForce GTX660 2GB or above		
Hard Drive	SATA 7200 RPM, 500 GB or above		
Network	1 Gbps or above		
VMS Server Only			
OS	64-bit : Windows 7 Professional, Enterprise, Ultimate		
CPU	Intel Core i3-530 or above		
Memory	4 GB or above		
Display	On board (generic) 256MB or above		
Hard Drive	SATA 7200 RPM, 500 GB or above		
Network	1 Gbps or above		

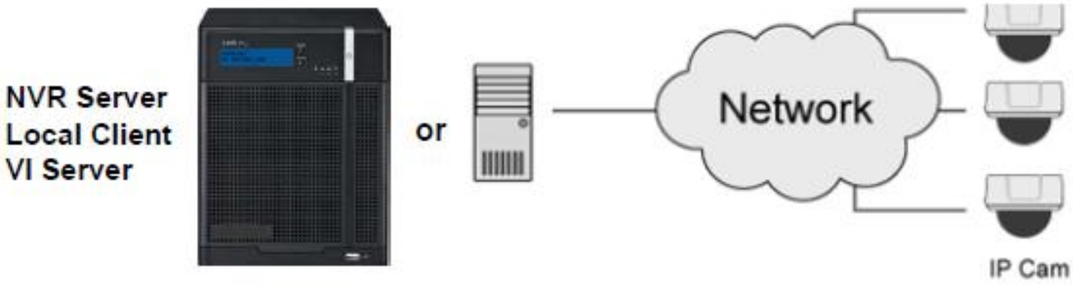
3.3.1. Standalone Server (Client-Server All-in-One)

For users with standalone Server, the Local Client UI is used to manage NVR Server services:


Local Client UI
Local Domain Server
User/Resource Mgmt
SMR/NVR/VMS Server
Recording Server
Video Streaming
Alarm Events Handling
(Optional) VI Server
1. Authentication through Local Domain Server
2. Success, access to SMR/NVR/VMS Server Services
*VI receives images from VMS Server for Video Analytic activities.
In case of events, it will return warning back to VMS Server.

※Application:

The Server, IP cameras are all in the same LAN.



Use NVR as Server

No installation needed.

Use PC as Server

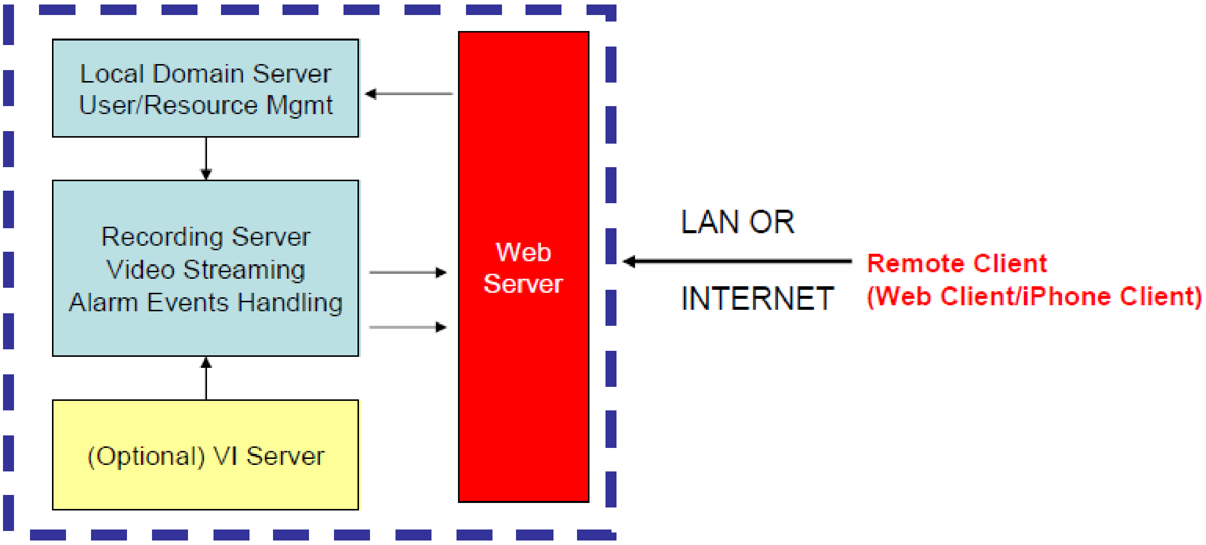
Install both the VMS/NVR Server and VMS Client on a PC:

①Insert the VMS/IPCAM product CD. ②Click **VMS Suite** on the menu to start the installation. ③Choose *Typical Setup*. If you don’t need video analytic functions, *Advanced Setup* can be selected to uncheck the VI Server.

3.3.2. Standalone Server + Remote Client (Web Client / SPhone Client)

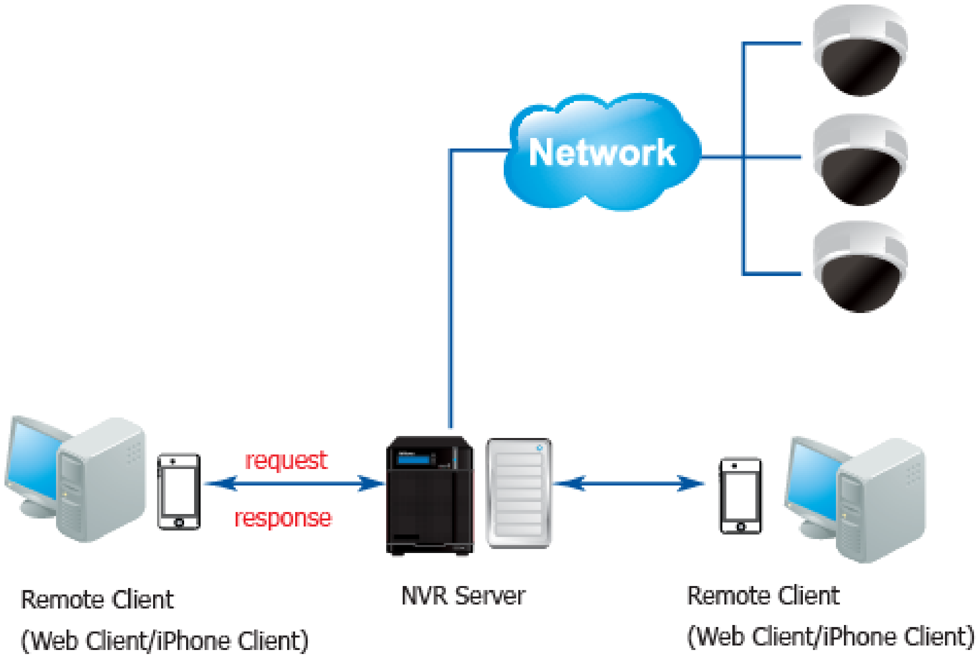
For remote users to connect to SMR/NVR Server, a remote access, VMS Client installed on remote PCs is needed for live video monitoring, event recording playback access.

Also, the Web Client, an ActiveX application (OCX) can be used for basic live viewing and event playbacks through the web browser, while SPhone Client can be used for basic live viewing on iPhone/Android devices.



Application1: Internet

The Server, IP cameras and the PC/Mobiles are all in the same LAN.



[NVR Server]

Use SMR/NVR as Server

No installation needed.

Use PC as Server

Install the VMS/NVR Server on a PC:

① Insert the VMS/IPCAM product CD.

②Click **VMS Suite** on the menu to start the installation.

③Choose *Advanced Setup* to uncheck the VMS Client.

If you don't need video analytic functions, the VI Server can also be unchecked.

Install the Web Server on the PC:

① Insert the VMS/IPCAM product CD.

②Click **Browse CD/DVD** in the menu.

③Double click **WebServerSetup.exe** to start the installation**.**

[Client]

Install the VMS Client on PCs:

①Insert the NVR/SMR product CD.

②Click **VMS Client** on the menu to start the installation.

Install the Web Client on the PCs (Optional):

Launch Microsoft Internet Explorer 7.0 (or above) and enter your **VMS Server IP address + "/webclient"** in your web browser's URL location, eg. http://172.18.6.9/webclient to download the Web Client application.

Install the SPhone Client (Optional):

Download the SPhone Client from App Store on the iPhone desktop.

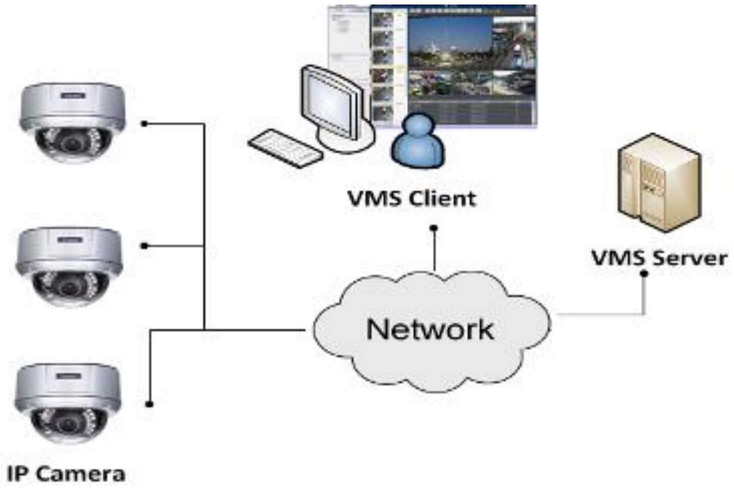
Install the SPhone Client (Optional)

Download the SPhone Client from App Store on the Andriod phone desktop.

Note: Please refer to *Installing the VMS and Installing the Web Client* for details.

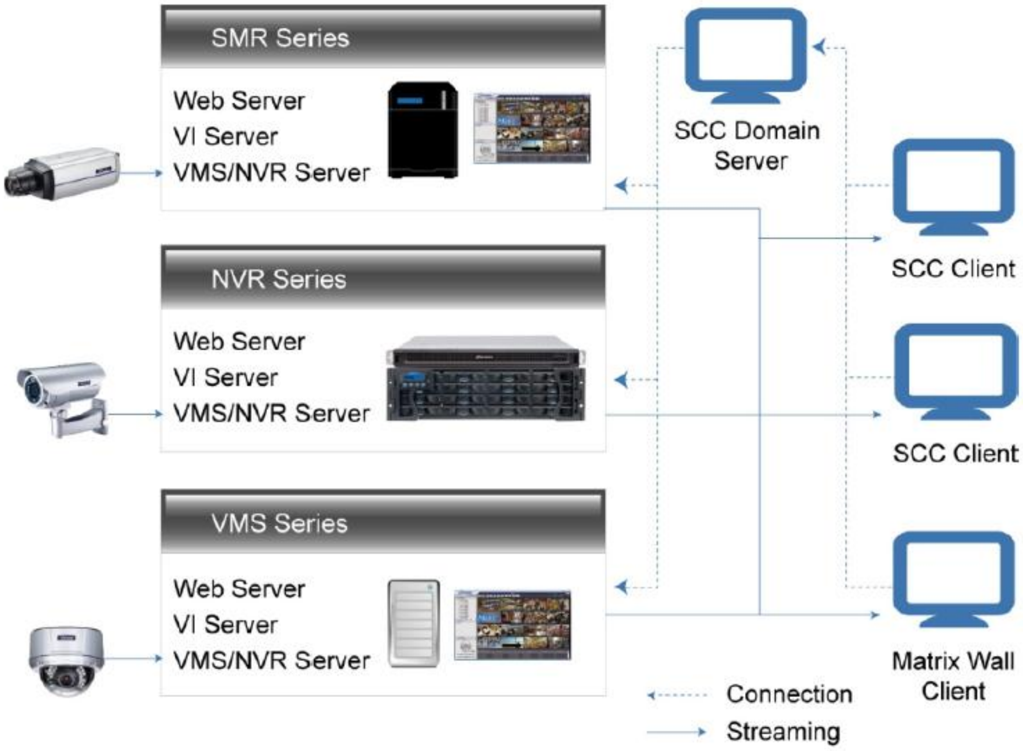
Application 2: Internet

The Server, some of the IP cameras and the PC are all in the same LAN, while the other IP cameras are installed in remote location with Public IP.



3.3.3. Multiple Servers + SCC Client

For users with multiple SMR/NVR Servers, SCC Client UI is used to manage over the domain infrastructure.

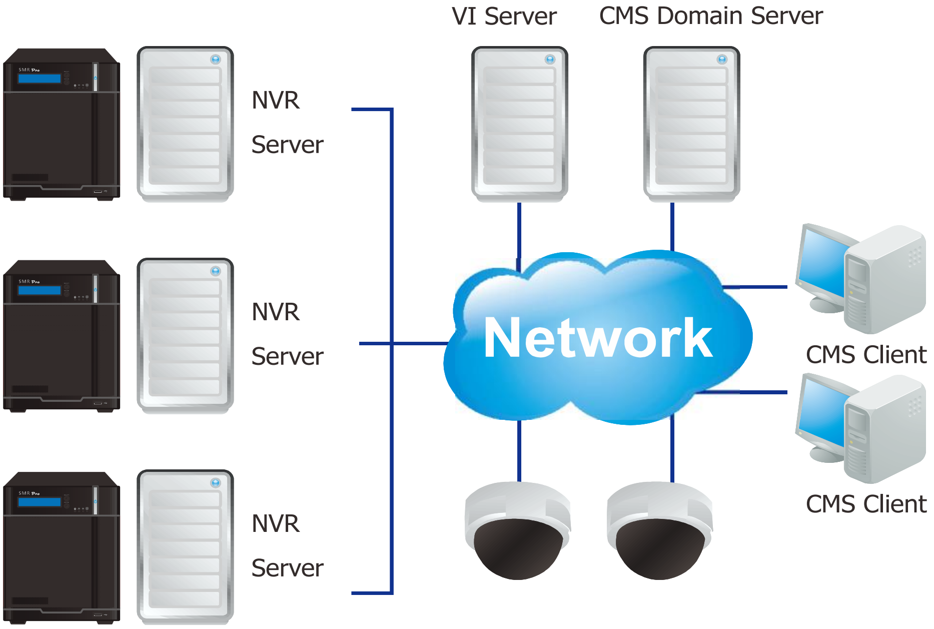


Application3: Internet

(1) The Servers, IP cameras and the PCs are in LAN A.

(2) Some IP cameras are installed in LAN B, which is behind a different router in a remote location.

(3) Users are allowed to connect the SMRs/NVRs from remote PC over the Internet.



[NVR Server]

Use SMR/NVR as Server

No installation needed.

Use PC as Server

Install the VMS/NVR Servers on PCs:

①Insert the VMS/IPCAM product CD.

②Click **VMS Suite** on the menu to start the installation.

③Choose *Advanced Setup* to uncheck the VMS Client.

The VI Server can also be unchecked, if you don't need video analytic functions.

[VI Server] (Optional)

You can choose to install the VI Server only on a standalone PC to manage the video intelligence data.

①Insert the VMS/IPCAM product CD.

②Click **VMS Suite** on the menu to start the installation.

③Choose *Advanced Setup* to choose VI Server only.

[SCC Domain Server]

Install the SCC Domain Server on a PC:

①Insert the NVR/SMR product CD.

②Click **SCC Suite** on the menu to start the installation.

③Choose *Advanced Setup* to select the SCC Domain Server only.

[SCC Client]

Install the SCC Client on PCs:

①Insert the NVR/SMR product CD.

②Click **SCC Suite** on the menu to start the installation.

③Choose *Advanced Setup* to select the SCC Client only.

Note: (1) For users don’t have Surevon SMR/NVR series, please contact your dealer for the SCC installation file. (2) The SCC Domain Server can also be installed together with the SCC Client in the same PC by choosing *Typical Setup*. (3) Please refer to *Installing the VMS* and *Installing the SCC* for details.

3.3.4. Network Requirements

In order to preserve enough bandwidth for surveillance video, a surveillance network is presumed to be free of user/business traffic. Server software currently supports Class B and Class C type addresses. Currently the Server software only searches for Servers on the same subnet. Cameras should also reside on the same subnet.

Opening Ports

If access through a firewall in a local network is required, try opening the following ports: SMTP (25), HTTP (80), FTP (20, 21), OMNI (2809), HTTPS (443) and RTSP (554, 8554.). Other ports should also be opened while using port forwarding to access the VMS Server: Stream Port (9090), Doman Data Port (9060), Log Download Message Port (15507) and Log Download Data Port (9080).

Access through a firewall	Use port forwarding to access
SMTP (25), HTTP (80), FTP (20, 21), OMNI (2809), HTTPS (443), RTSP (554, 8554.)	Stream Port (9090), Doman Data Port (9060), Log Download Message Port (15507), Log Download Data Port (9080)

Note: Please refer to *Port Forwarding* Section for more details.

Warnings / Precautions

If the Server and a VMS client reside on separate subnets, please set up gateway, VLAN, or cross-subnet routing to bridge surveillance traffic. Please consult with a network administrator for problems with network setups. A VMS client needs to be rebooted when network settings are changed.

3.4. Port Forwarding

Port forwarding is a name given to the combined technique of:

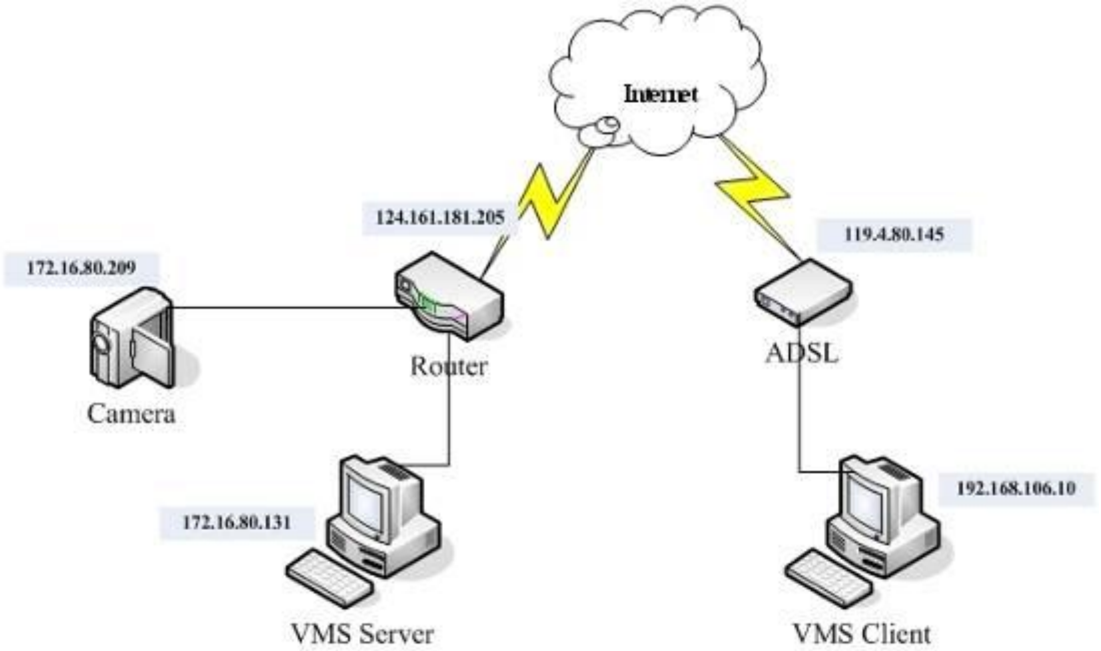
1. Translating the address and/or port number of a packet to a new destination.
2. Possibly accepting such packet(s) in a packet filter (firewall).
3. Forwarding the packet according to the routing table.

To illustrate its concept, two computers on the Internet that communicate with each other using TCP/IP or UDP/IP protocols(though the process is not limited to these) utilize ports to identify the opposite connection points of each other where the data packets supposed to go to. In order to communicate, each computer knows the port of another computer (in addition to IP address) and sends the data to that port. Port forwarding forwards these ports in such a way that when one computer sends data to the specific port of another computer, the data is actually sent to a different port. This allows remote computers to connect to a specific computer or service within a private LAN.

In a typical residential network, nodes obtain Internet access through a DSL or cable modem connected to a router or network address translator (NAT/NAPT). Hosts on the private network are connected to an Ethernet switch or communicate via a wireless LAN. The NAT device's external interface is configured with a public IP address. The computers behind the router, on the other hand, are invisible to hosts on the Internet as they each communicate only with a private IP address.
When configuring port forwarding, the network administrator sets aside one port number on the gateway for the exclusive use of communicating with a service in the private network, located on a specific host. External hosts must know this port number and the address of the gateway to communicate with the network-internal service.

When used on gateway devices, a port forward may be implemented with a single rule to translate the destination address and port. The source address and port are, in this case, left unchanged. When used on machines that are not the default gateway of the network, the source address must be changed to be the address of the translating machine, or packets will bypass the translator and the connection will fail.

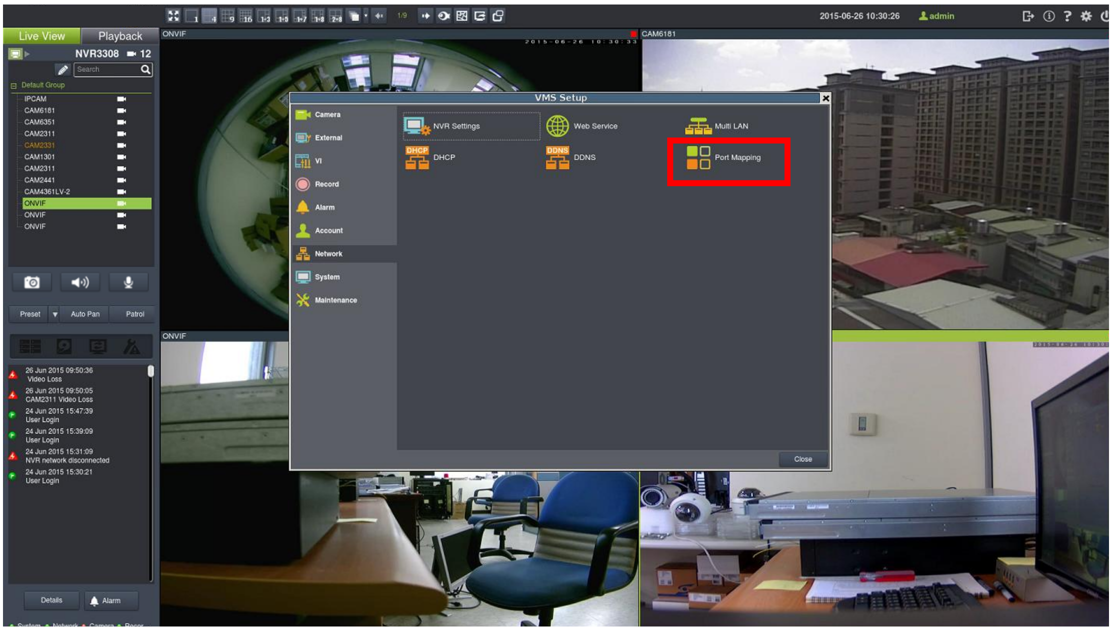
3.4.1. Port Forwarding for Accessing VMS Server



To enable port forwarding for accessing VMS Server, please follow the steps below:

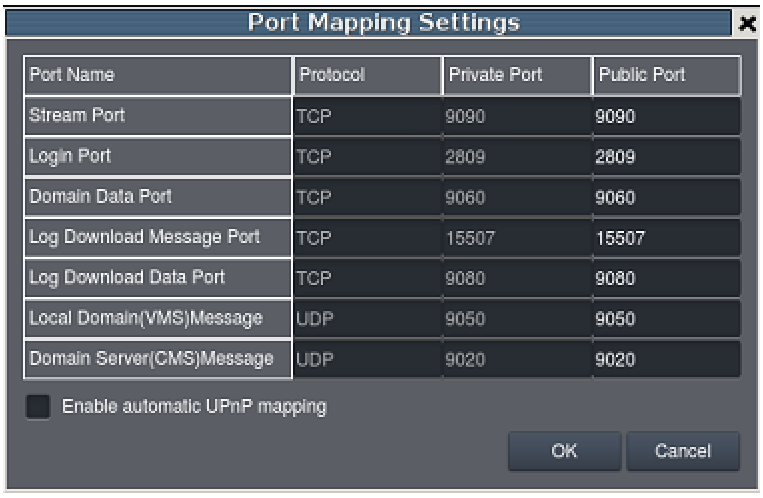
1. Do Router Port Mapping for VMS/NVR Server

   Go to ***VMS Setup*** > ***Network*** > ***Port Mapping*** in VMS after it is installed.



```
26 Jun 2015 09:50:36
 Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected
24 Jun 2015 15:30:21
User Login
```

A *Router Port Mapping* window will prompt for entering port numbers. Please put in the numbers as listed below:



Port Mapping Settings

Port Name	Protocol	Private Port	Public Port
Stream Port	TCP	9090	9090
Login Port	TCP	2809	2809
Domain Data Port	TCP	9060	9060
Log Download Message Port	TCP	15507	15507
Log Download Data Port	TCP	9080	9080
Local Domain(VMS)Message	UDP	9050	9050
Domain Server(CMS)Message	UDP	9020	9020

□ Enable automatic UPnP mapping

Stream Port: 9090

Login: Port: 2809

Doman Data Port: 9060

Log Download Message Port: 15507

Log Download Data Port: 9080

2. Open Ports on the Router

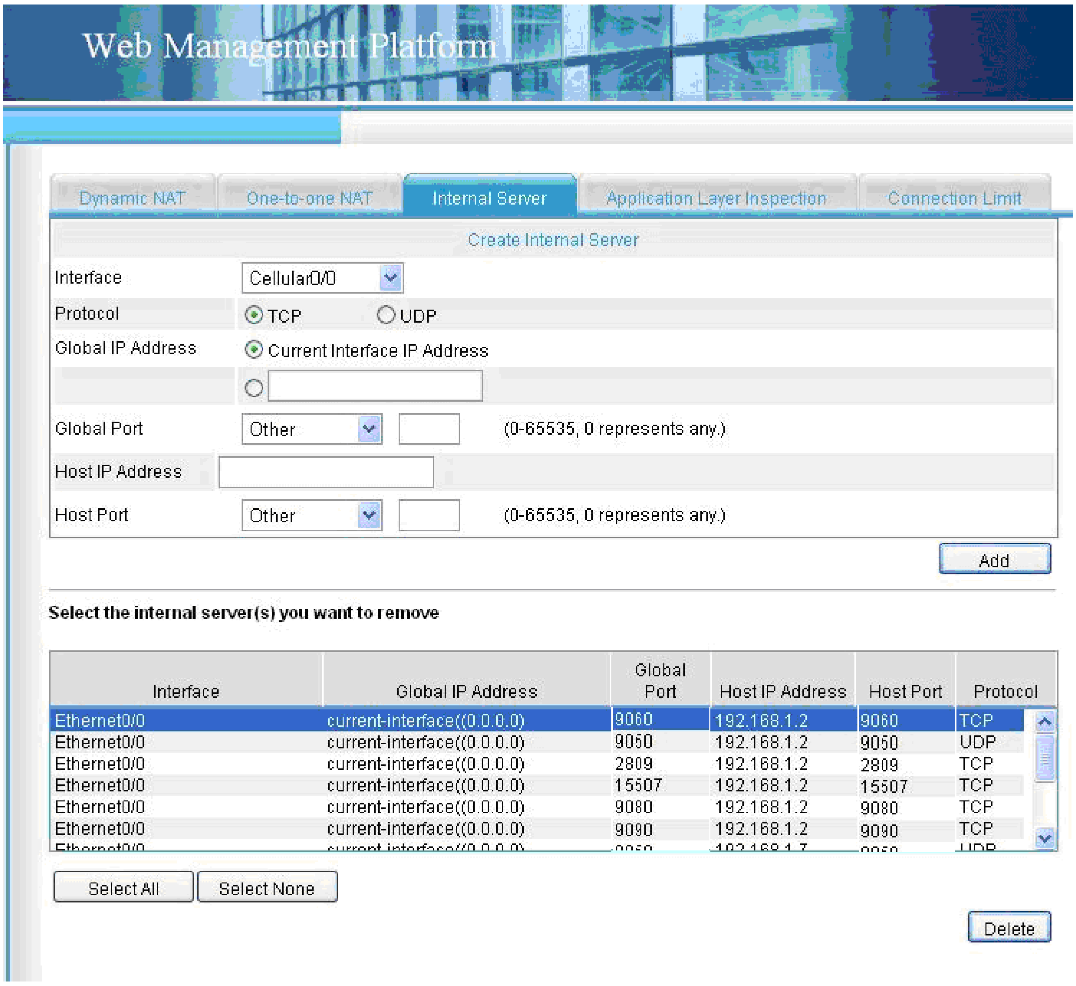
Host Ports: The private ports that the internal VMS/NVR Server use, which are unchangeable.

Global Ports: The public ports for remote clients to connect to the internal VMS/NVR Server. The Global ports are changeable, but the simplest way is to make them the same with the host ports.

Please open the listed ports on your router:

(When the option “Enable Automatic Upnp Mapping” is selected, this step can be skipped.)

Port(Host/Global Port)	Protocol	Port Number
Domain Message Port	UDP	9050
Domain Data Port	TCP	9060
Login Port	TCP	2809
Stream Port	TCP	9090
Log Download Message Port	TCP	15507
Log Download Data Port	TCP	9080



Create Internal Server

Interface	Cellular0/0
Protocol	● TCP ○ UDP
Global IP Address	● Current Interface IP Address ○
Global Port	Other (0-65535, 0 represents any.)
Host IP Address	
Host Port	Other (0-65535, 0 represents any.)

Select the internal server(s) you want to remove

Interface	Global IP Address	Global Port	Host IP Address	Host Port	Protocol
Ethernet0/0	current-interface((0.0.0.0)	9060	192.168.1.2	9060	TCP
Ethernet0/0	current-interface((0.0.0.0)	9050	192.168.1.2	9050	UDP
Ethernet0/0	current-interface((0.0.0.0)	2809	192.168.1.2	2809	TCP
Ethernet0/0	current-interface((0.0.0.0)	15507	192.168.1.2	15507	TCP
Ethernet0/0	current-interface((0.0.0.0)	9080	192.168.1.2	9080	TCP
Ethernet0/0	current-interface((0.0.0.0)	9090	192.168.1.2	9090	TCP

Note: Camera port (default: 80) and stream port (default: 6002) for accessing cameras should be opened while VMS/NVR Server and the cameras and are not in the same LAN.

Chapter 4. Installation

4.1. Before You Start

4.1.1. Checklist for Operating Environment

Users need to prepare the following devices to set up the surveillance system.

Network Video Recorder	NVR5000 series
IP Camera	Network Cameras (such as CAM2441)
Network	Existing LAN, Switch, Router or Hub (please see the Network Topology below)
Storage	Hard Drives

Note: The hard drives should be purchased separately.

4.1.2. Checklist for Network Topology

Make sure you have the right switch/hub for your environment. Either of the following options will work.

	Common Topology	Reference Product
Existing LAN	LAN Switch with DHCP Server	Office LAN
Router	LAN Switch with build-in DHCP Server	D-Link DIR-130
Switch/Hub	No DHCP Server(refer to the Note below)	D-Link DES-1108

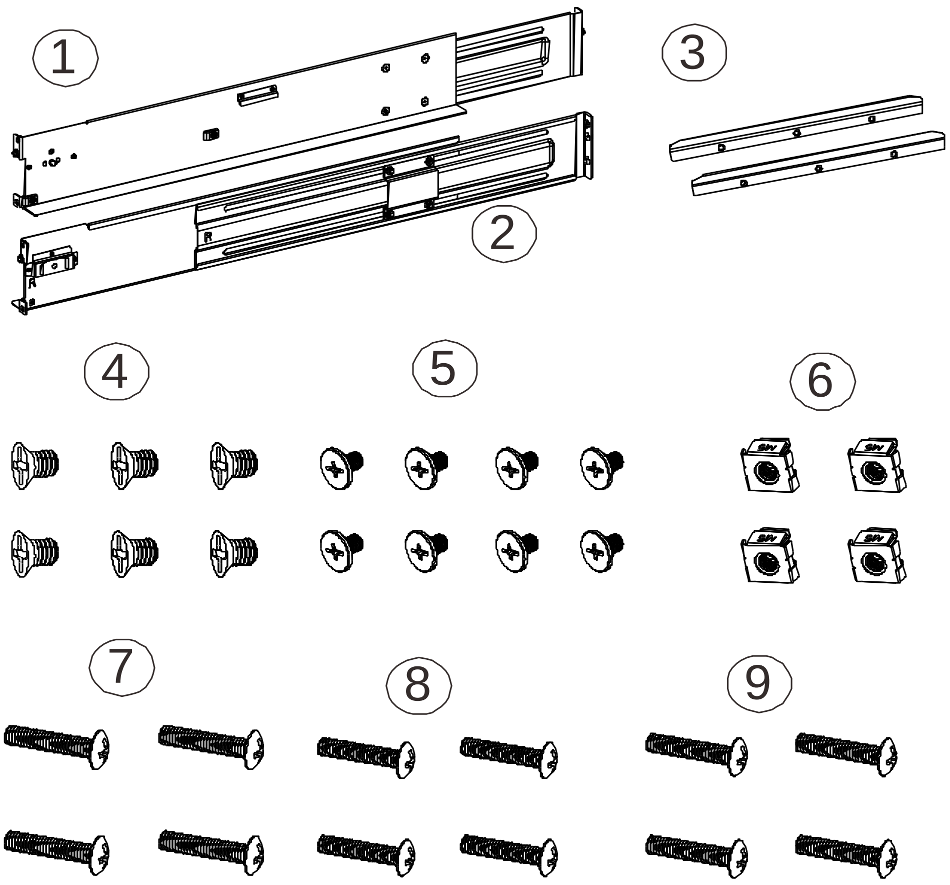
Note: For devices without DHCP Server function, please refer to Configuring DHCP Service Section.

4.2. Slide Rail

4.2.1. Slide Rail Kit Contents

The following table shows all accessories that came with the slide rail kit.

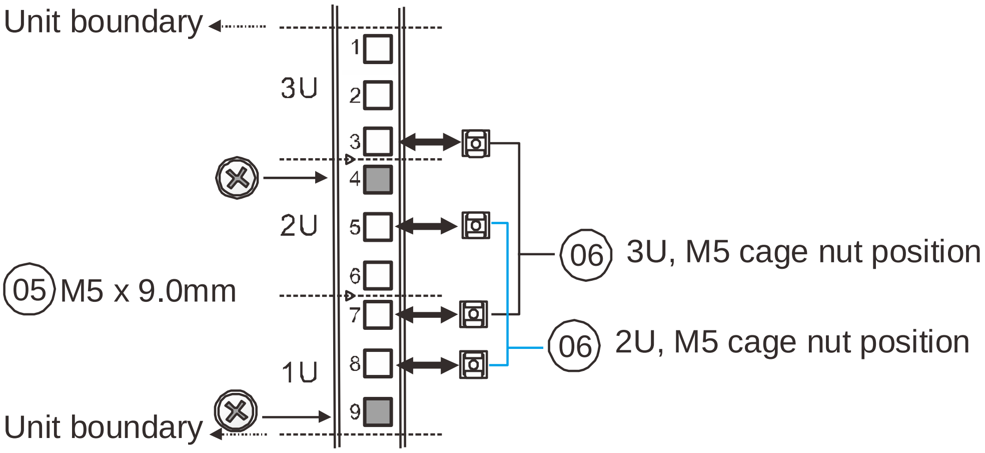
Item	Description	Quantity
01	Mounting bracket assembly, left-side	1
02	Mounting bracket assembly, right-side	1
03	Inner glides	2
04	Flathead screws #6-32 L4	6
05	Truss head screws M5 x9.0mm	8
06	M5 cage nuts	4
07	M5 x 25mm	4
08	M6 x 25mm	4
09	#10-32 x 25.4mm	4



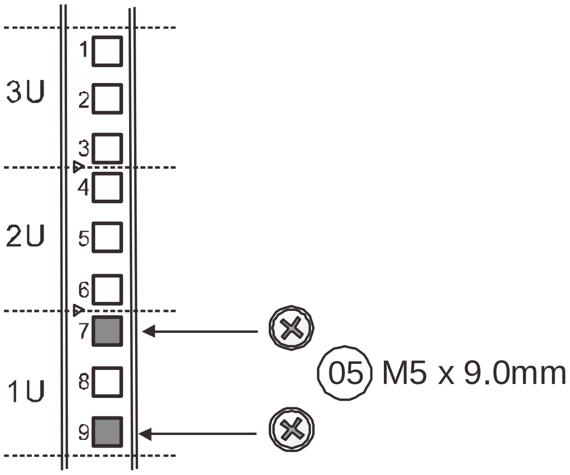
4.2.2. Installation Procedure

1. The installation begins with determining the installation position (front and rear rack positions) and M5 cage nut **(5)** insertion location.

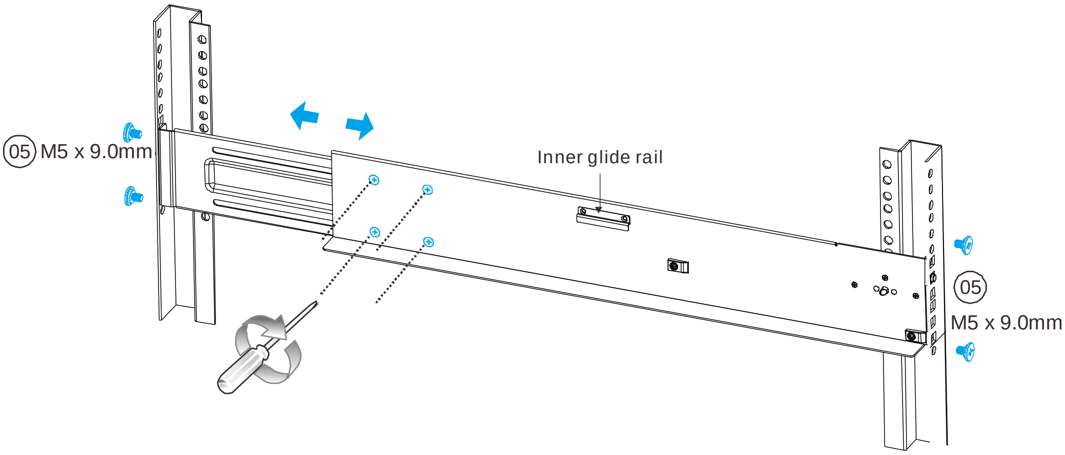
Front rack posts



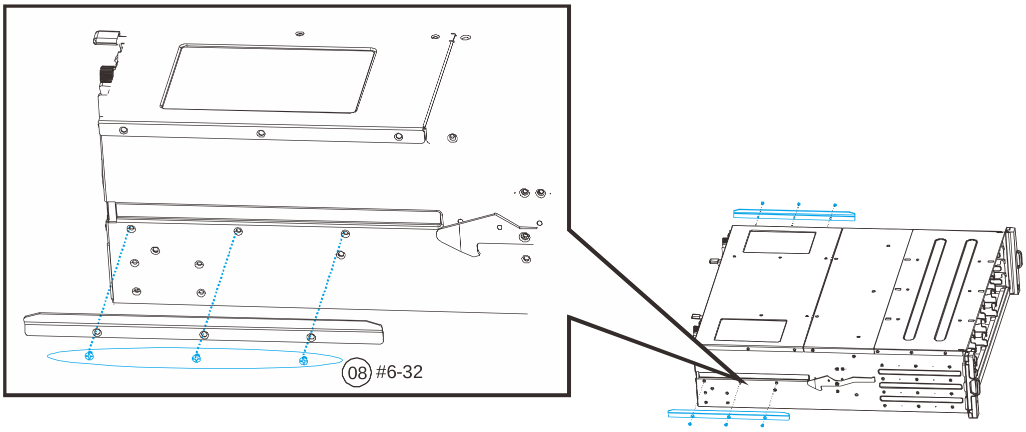
Rear rack posts



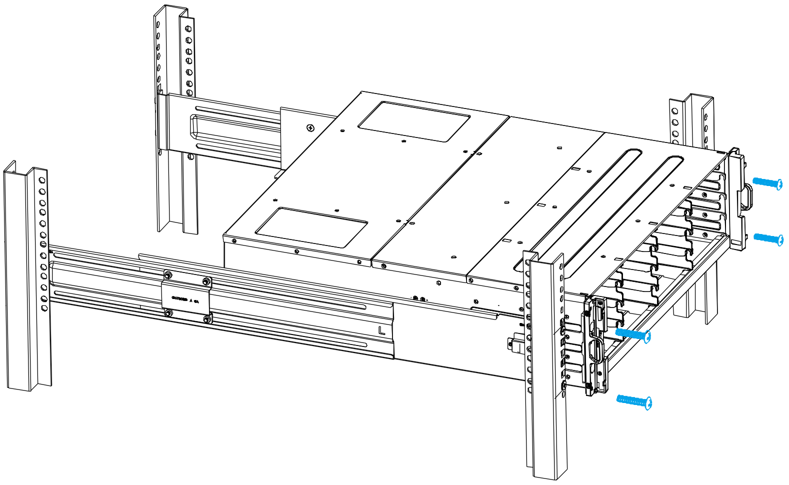
2. Adjust the length by loosening the four screws on the slide rail. Secure the slide rails to front and rear posts using truss head screws. Tighten the four screws on the slide to fix the length.



3. Attach inner glides to BOTH sides of the enclosure using flathead screws #6-32 **(8)**



4. With the assistance of another person, lift and insert the enclosure onto the slide rail. Make sure the inner glides on both sides of the enclosure meets the inner glide rail. Secure the enclosure with M5 or M6 screws from the front.

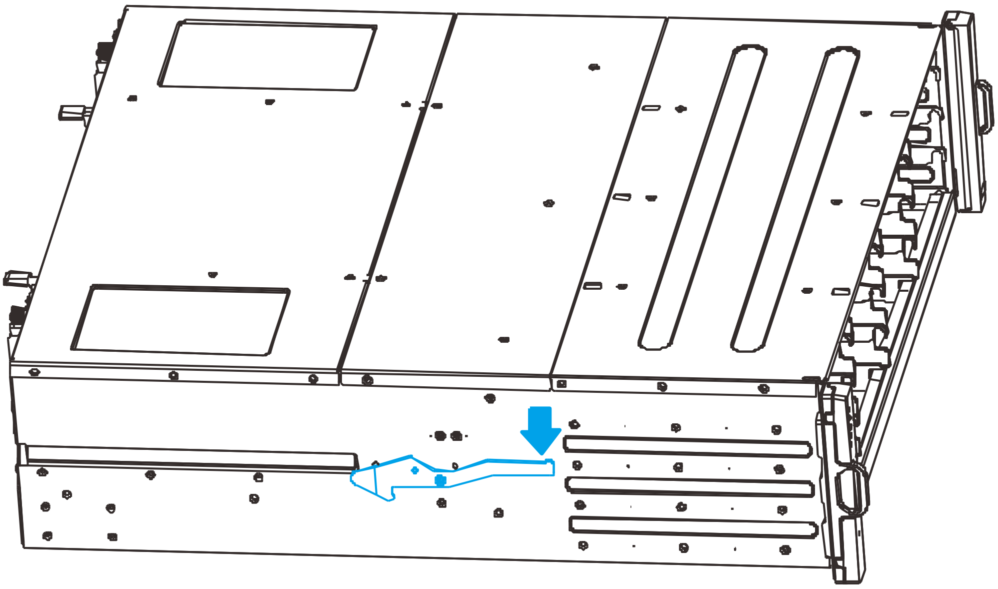


4.2.3. Removing the Enclosure

* Prior to removing the enclosure, power down your system (stop all I/O actions, please refer to Users' manual) and all hard drives have been removed!

* It is strongly recommended that two people work together on this procedure.

To remove the enclosure, make sure the system has been turned off, all cables have been disconnected and all hard drives have been removed. Gently pull the system out on the slide rail until it has reached it's full extension on the rail, a hook (in blue) can be located on the left side of the enclosure, gently push down in the direction of the blue arrow to disengage the enclosure from the slide rail and pull out the enclosure.



4.3. Hard Drives Installation

Hard disk drives are purchased separately. When selecting hard disk drives (HDD), HDD manufacturers always urge users to choose enterprise/surveillance grade drives for 24/7 surveillance operations to ensure system stability. The surveillance hard drives on our Approved Vendor List (AVL) are engineered to work continuously, withstand high-temperature fluctuations and equipment vibrations found in any typical surveillance application. To reduce errors occurred on your RAID data and the chance of the recording performance being affected, it is highly recommended to use HDDs listed on our Approved Vendor List (AVL) to ensure reliability. Find the AVL on our web page: http://www.surveon.com/support/hardware.asp

4.3.1. Prerequisites

Capacity (MB/GB): Use hard drives that have the same capacity and rotation speeds. RAID arrays use a "least-common-denominator" approach meaning the maximum capacity used in each drive for comprising a logical configuration is the maximum capacity of the smallest drive. Profile: The enclosure drive bays are designed for 3.5-inch wide x 1-inch pitch hard drives.

Drive Interface Type: The enclosure accommodates SATA-II (3Gbps) or SATA-III (6Gbps) hard drives.

Note: The hard drives and drive trays should only be installed into the system after it has been mounted into a rack cabinet. If the hard drives are installed first, the system will be too heavy to handle and the possible impact during installation may damage your hard drives.

Users **MUST** install at least **ONE** hard drive into slot 1 to setup the system. It is strongly recommended to install at least **TWO** hard drives upon initialization!

OS hard drives: Enclosure slots 1 & 2 are for OS dedicated hard drives. It is recommended that the two hard drives are of the same brand, capacity, rotational speed and model.

RAID Configuration: Below is a list of the level of fault tolerance for different RAID levels:

RAID Level	Max. No. of Failed Drives without Data Loss
0	No fault tolerance. 1 drive fails and the data is lost.
1	1 (mirrored pair)
5	1
6	2

SAS / SATA hard drive for storage: It is recommended to use hard drives that are of the same brand, capacity, rotation speed and same model in an enclosure. RAID arrays use a “least-common-denominator” approach meaning the maximum capacity used in each drive for comprising a logical configuration is the maximum capacity of the smallest drive. **Profile**: The enclosure drive trays are designed for 3.5-inch wide x 1-inch pitch hard drives.

Note: Hard drives dedicated for OS will have certain storage capacities that are unavailable for use towards the total storage capacity.

⚠ WARNING

Make sure all enclosure tray slots are filled a hard drive tray (with or with a hard drive) as an empty tray slot may affect the airflow efficiency of the enclosure!

The hard drives should only be installed into the system **AFTER** the enclosure has been rack mounted as the combined weight will be too heavy to handle.

Handle hard drives with extreme care and observe all ESD prevention methods when installing drives.

Only use screws supplied with the system package. Longer screws may damage the hard drives or its trays.

4.3.2. Hard drive Designation

The general alignment is from left to right and/ or top to bottom in numeric order as shown below.

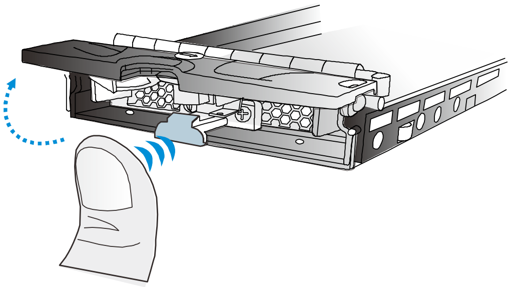
Hard Drive Slot 1	Hard Drive Slot 2	Hard Drive Slot 3	Hard Drive Slot 4
Hard Drive Slot 5	Hard Drive Slot 6	Hard Drive Slot 7	Hard Drive Slot 8
Hard Drive Slot 9	Hard Drive Slot 10	Hard Drive Slot 11	Hard Drive Slot 12
Hard Drive Slot 13	Hard Drive Slot 14	Hard Drive Slot 15	Hard Drive Slot 16

WARNING

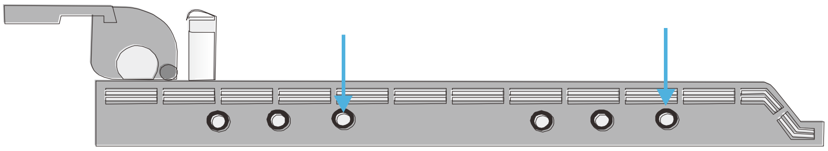
Tray numbering sequence is important because if any faults occur to disk drives, you need to identify the location of the faulty drive(s). For example, if you mistakenly remove 2 drives from a RAID5 logical drive, data will be lost.

4.3.3. Installing Hard Drive to the Tray

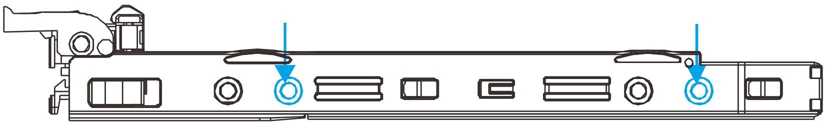
To remove the tray from the enclosure, press the release button and gently pull out the tray.



Place the hard drive into the drive tray. Make sure the hard drive is oriented that the drive's interface connector is facing the open side of the drive tray and its label side facing up. Adjust the drive's location until the mounting holes in the drive canister are aligned with those on the hard drive. Secure the drive with four (4) supplied 6/32 flathead screws.



Type I Tray

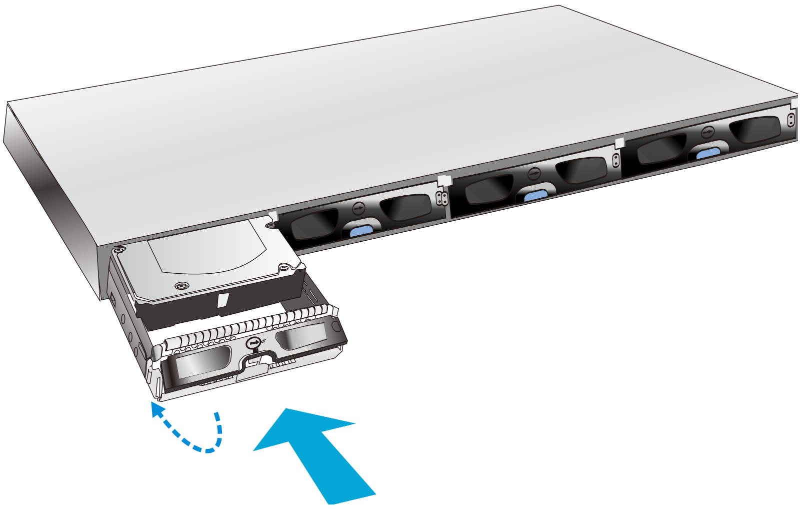


Type II Tray

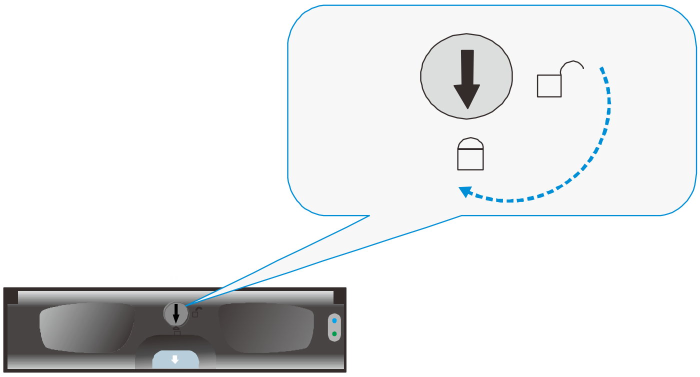
4.3.4. Installing the Drive Tray into the Enclosure

Once the hard drives have been installed in the drive trays, the drive trays are ready to be installed into the system.

With the tray bezel open, insert the installed hard drive and tray into the enclosure. Once inserted, close the tray bezel.



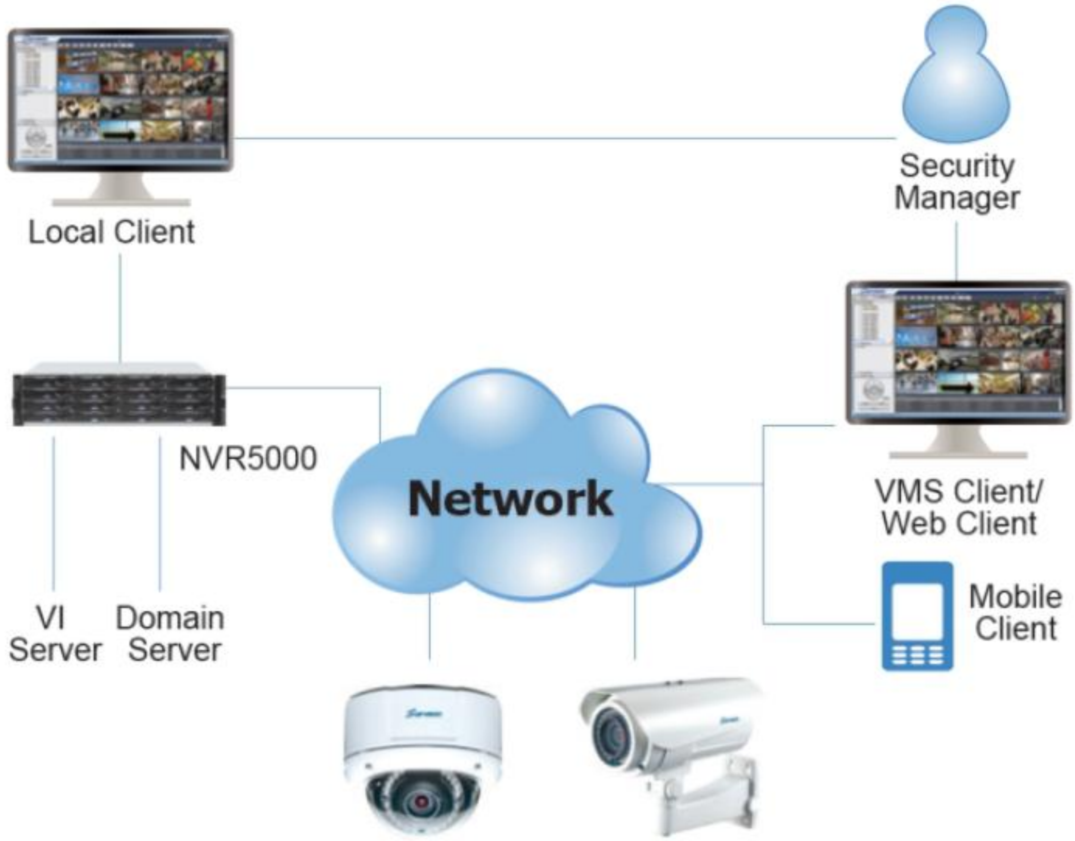
Use a small flathead screwdriver to rotate the tray bezel lock from the unlock position to the lock position.



4.4. Connections

4.4.1. System Connections for Initialization

Note: Make sure you have at least installed **ONE** hard drive into the system. It is strongly recommended to install at least **TWO** hard drives upon initialization!



The system connection requires the user to

(1) Connect an Ethernet cable from the system to a switch / router

(2) Place the CD that came with the system into your PC's CD-ROM

(3) Connect an Ethernet cable from the "**SAME**" switch / router to the PC

(4) Connect the power cable(s) to the system and to a power outlet

(5) Press the power button / switches to start up the system

4.4.2. System Connections for Initialization

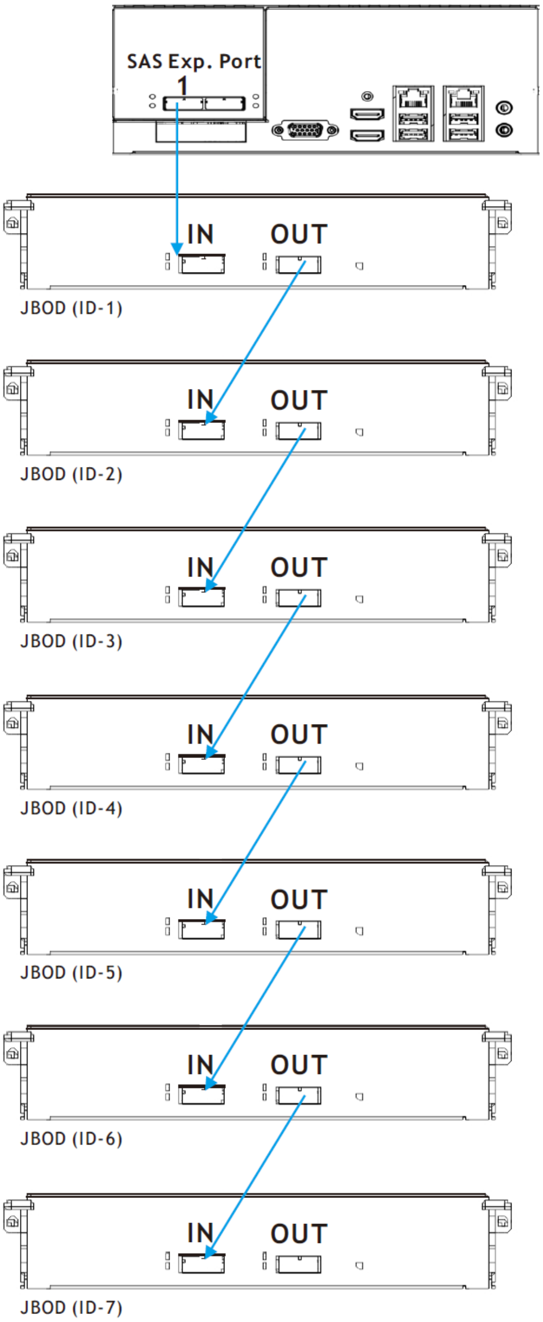
A SAS host link cable is included per JBOD. If you need to purchase other cables or if you need other cable(s) of different length, please contact your vendor.

The cable features include: 28AWG x 8 pair, 100ohm, black, UL approved, lead-free, 50cm, 120cm, or 170cm cable lengths, and connectors that can be secured to chassis using thumb screws or latching mechanism.

> ⚠ WARNING
> All SAS cables are sensitive and must be handled with care. To prevent interference within a rack system, the cable routing path must be carefully planned and the cables must not be bent.

Please contact your vendor for a list of compatible components!

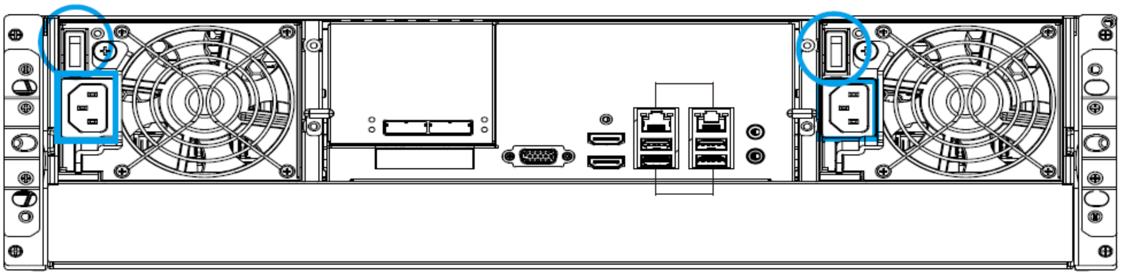
The following illustration is the recommended JBOD expansion connection; the maximum of JBOD expansion connection is up to 7 sets.



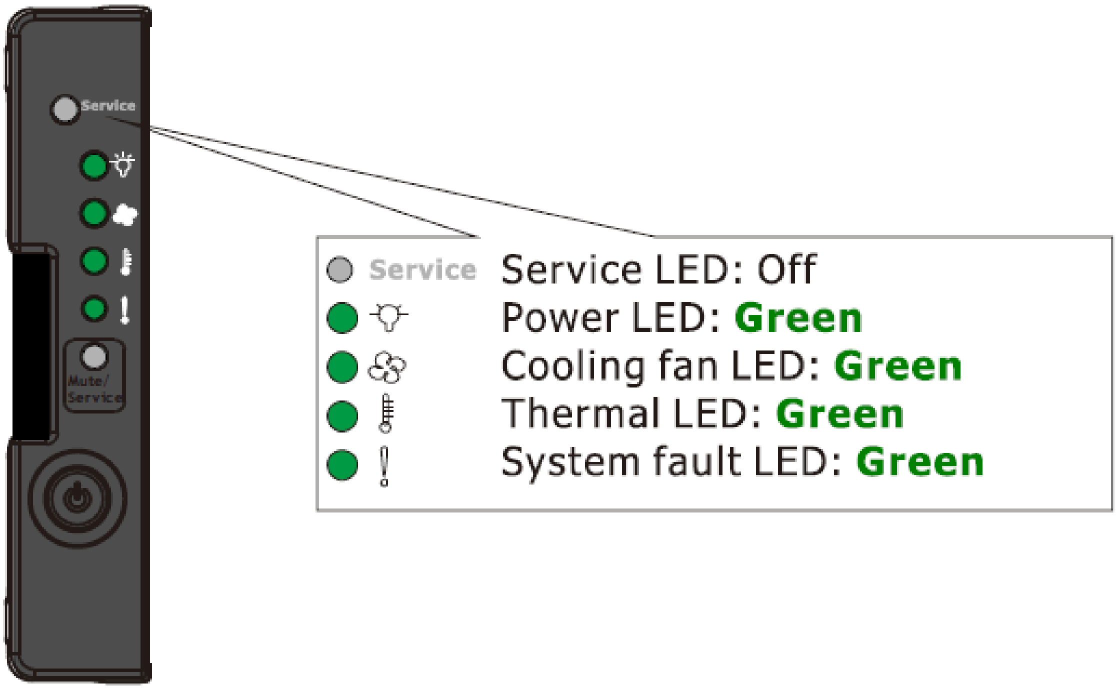
4.4.3. Status LED When Powered-on

1. Attach the power cable to the power socket (blue rectangles).

2. Press the power switch (blue circle).

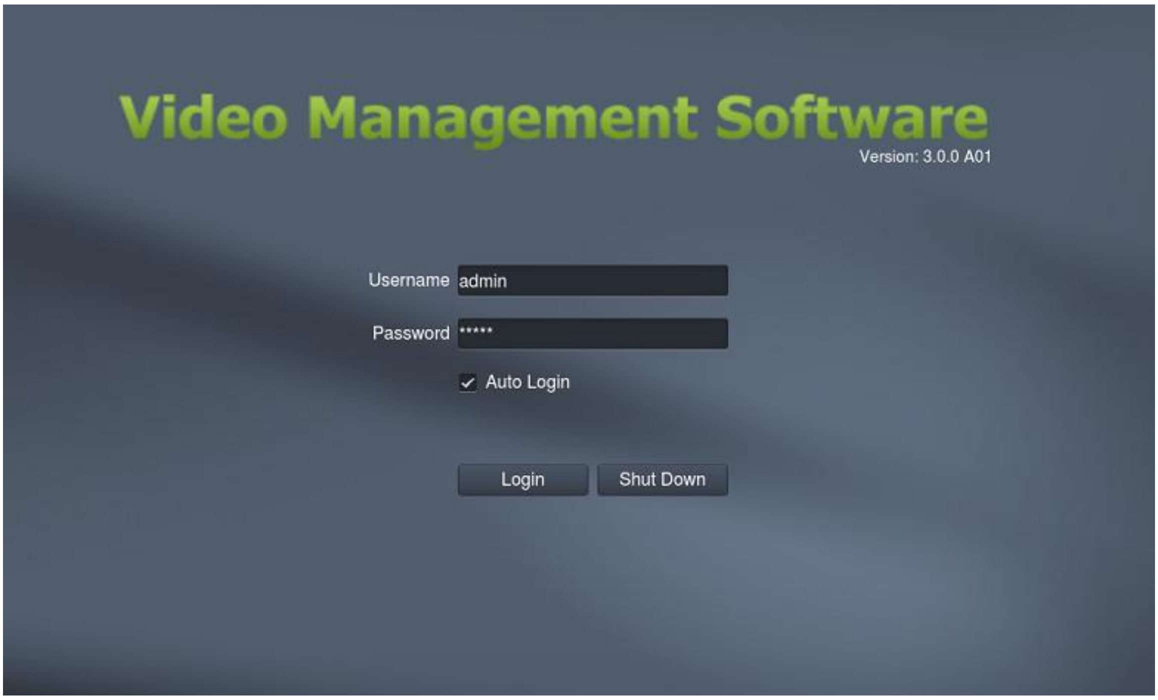


3. When turned on, the service LED should remain off while the rest of the status LEDs on the front panel should light up green to indicate normal operation.



4.5. Logging into NVR5000 Series

The Local Client will prompt for the following information after the NVR5000 Series system is powered on:



Username admin

Password *****

☑ Auto Login

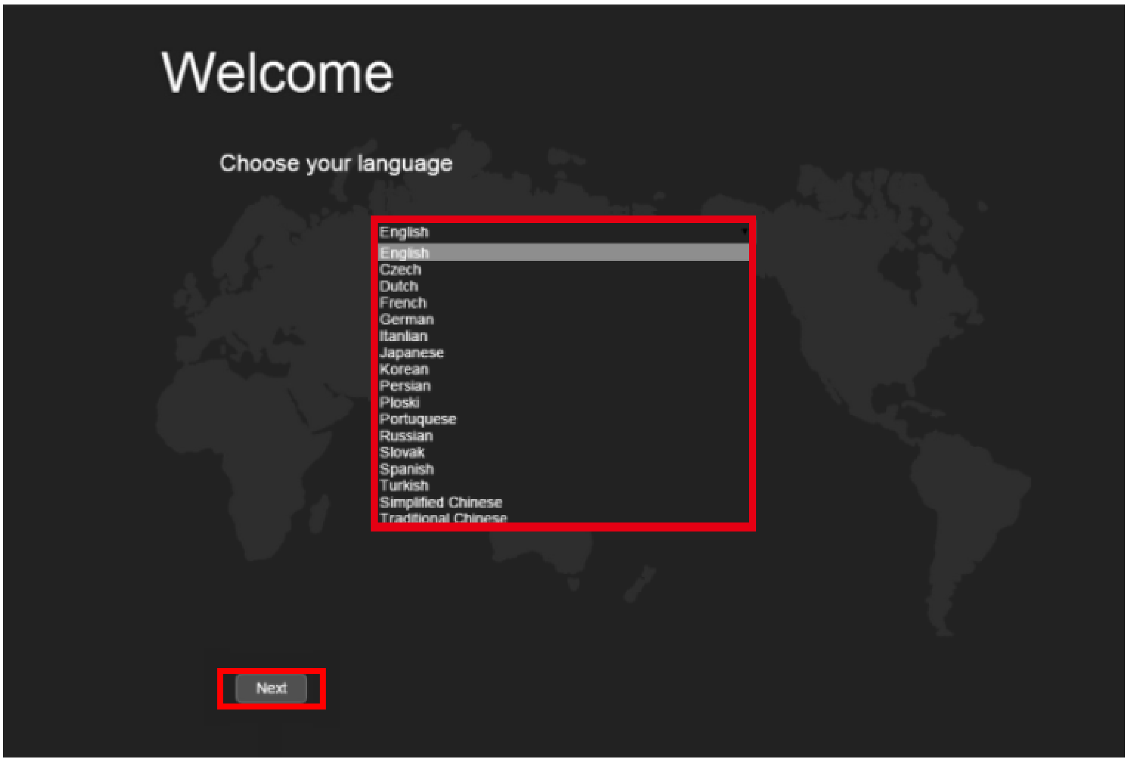
- **Username:** The username of the domain, which is always admin.
- **Password:** The password of the domain. Default password is admin.
- **Auto Login:** Check this option and you do not have to input the username and the password again when logging in next time.

Click Login after the password is entered.

4.6. Run the Install Wizard

When you run the NVR5000 series for the first time, you need to go through the following steps within the Install Wizard after logging in.

1. Welcome: Use the dropdown list to select the language for the VMS. Click **“Next”** to go to the next step **Confirm the number of your hard drives.**

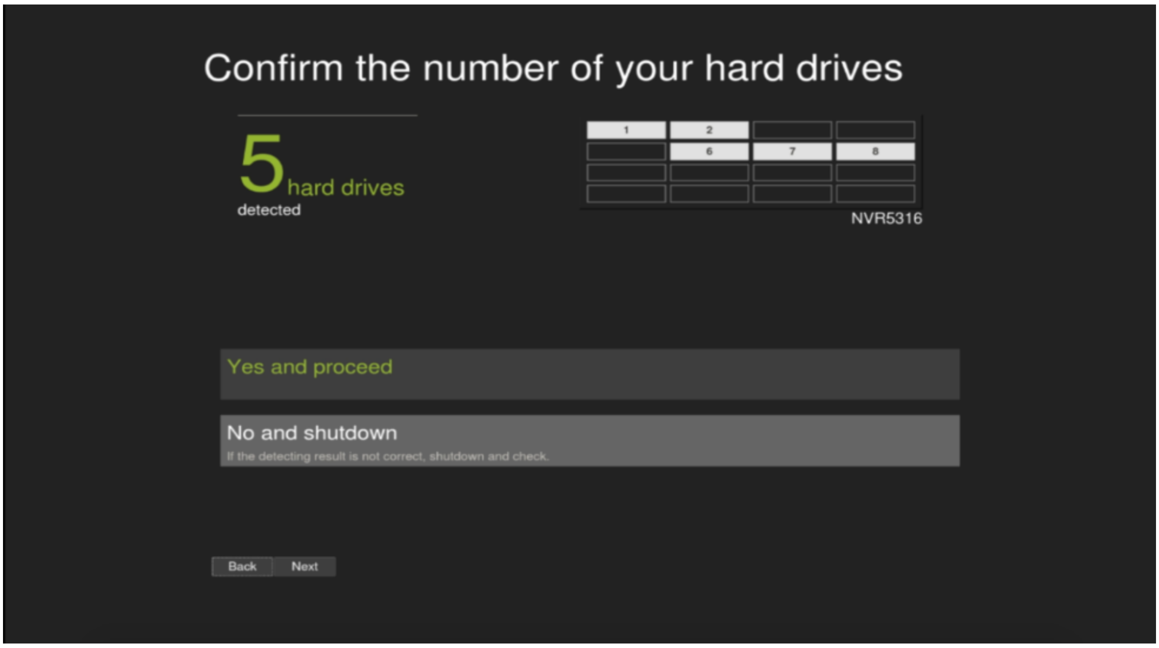


2. **Confirm the number of your hard drives:** the system will auto detect the number of installed hard drives.

Check if the detection result is correct, if yes, click ”**Yes and proceed**” or “**Next**” to go to the next step **Recording plan**.

If the detection result is not as expected, click ” No and shutdown” . Shutdown the system and make sure all the drives are installed properly. After checking, restart the system to run the install wizard.

Contact your system administrator, if this error keeps happening.



Confirm the number of your hard drives

5 hard drives detected

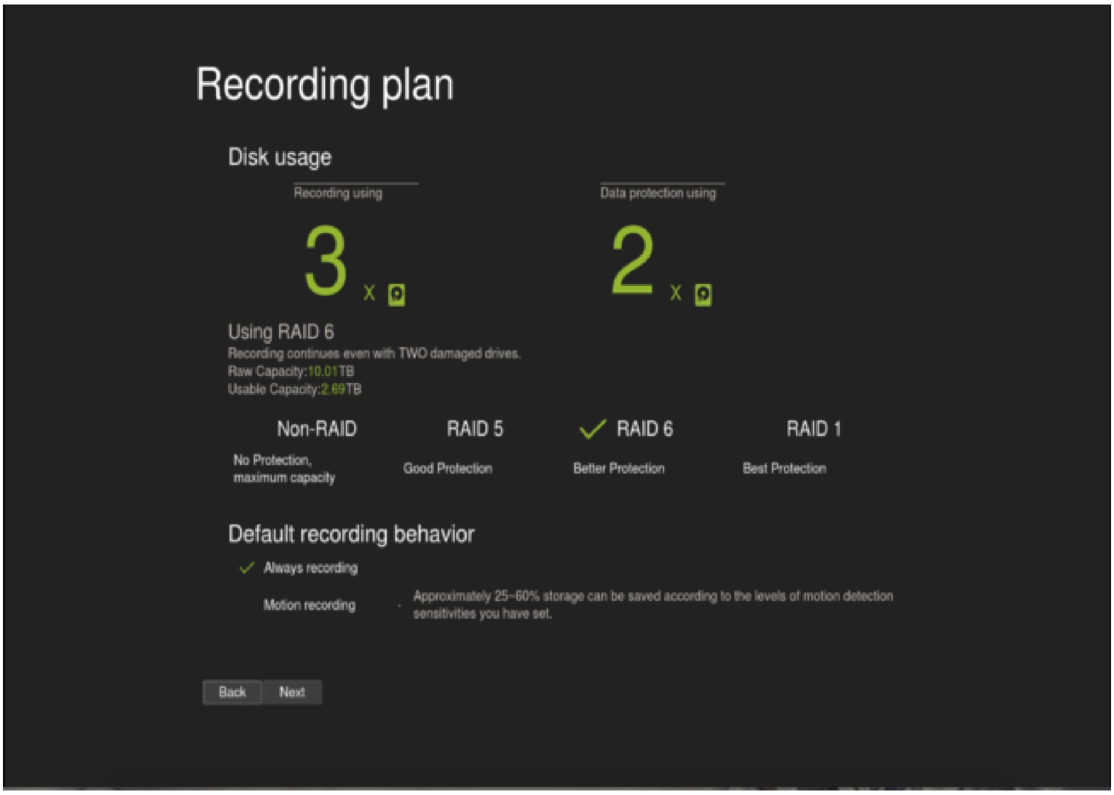
No and shutdown

If the detecting result is not correct, shutdown and check.

3. **Recording plan**: Select the best storage configuration for the system. See the following table for reference.

RAID Level			
RAID	**Description**	**Min. HDD**	**HDD Used for Storage**
Non-RAID	No protection, but maximum capacity.	2	All of HDDs
RAID 1	Best protection. Your data will be mirrored.	2	Half of HDDs
RAID 5	Use 1 disk to store the parity function data to provide fault tolerance.	3	HDD number minus 1
RAID 6	Used 2 disks to store the parity function data to provide fault tolerance.	4	HDD number minus 2

Please seek for professional help, if you are not sure how to select the RAID level.



Recording plan

Disk usage

Recording using 3 x

Data protection using 2 x

Using RAID 6

Recording continues even with TWO damaged drives.

Raw Capacity:10.01TB

Usable Capacity:2.69TB

Non-RAID — No Protection, maximum capacity

RAID 5 — Good Protection

✓ RAID 6 — Better Protection

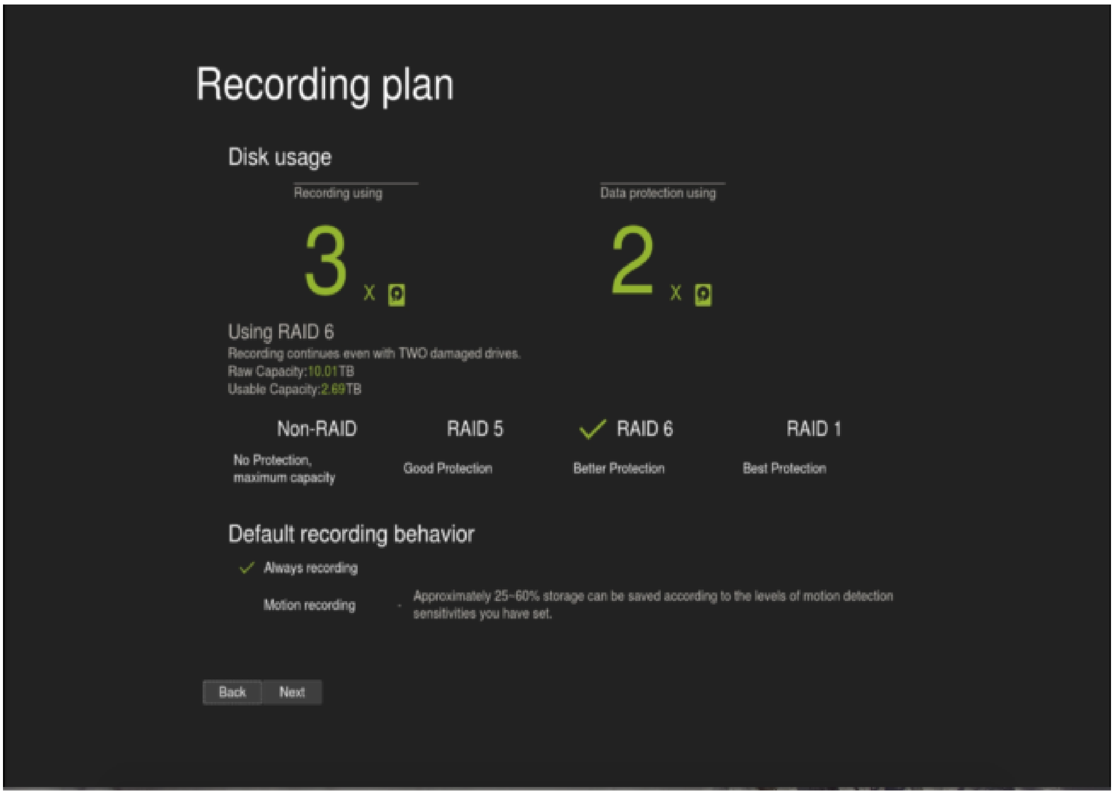
RAID 1 — Best Protection

Default recording behavior

✓ Always recording

Motion recording - Approximately 25~60% storage can be saved according to the levels of motion detection sensitivities you have set.

3.1. **Default recording behavior**: Select the best recording method. When **Always recording** is selected, every image will be recorded. When **Motion recording** is selected, only motion detected images will be recorded, and approximately 25~60% storage can be saved according to the levels of motion detection sensitivities you have set.



Recording plan

Disk usage

Recording using 3 x

Data protection using 2 x

Using RAID 6
Recording continues even with TWO damaged drives.
Raw Capacity:10.01TB
Usable Capacity:2.69TB

Non-RAID	RAID 5	✓ RAID 6	RAID 1
No Protection, maximum capacity	Good Protection	Better Protection	Best Protection

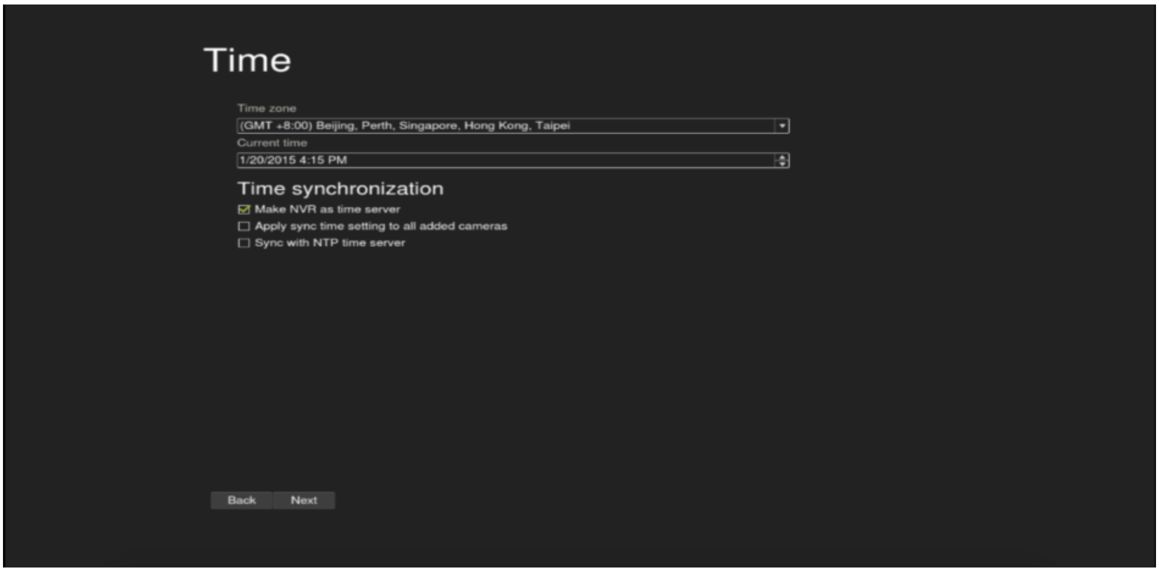
Default recording behavior

✓ Always recording

Motion recording - Approximately 25~60% storage can be saved according to the levels of motion detection sensitivities you have set.

Click “**Next**” to go to the next step **Time**.

4. Time: Time setup should be done correctly; otherwise some of the functions will be affected. Set up the time zone before setting up the time.



Time

Time zone

(GMT +8:00) Beijing, Perth, Singapore, Hong Kong, Taipei

Current time

1/20/2015 4:15 PM

Time synchronization

☑ Make NVR as time server

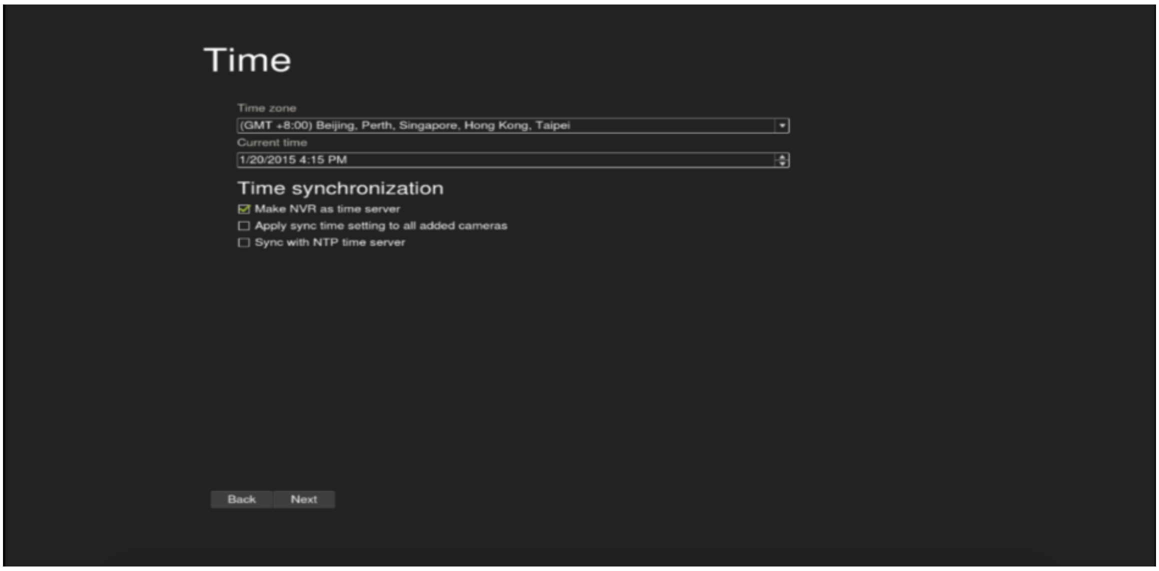
☐ Apply sync time setting to all added cameras

☐ Sync with NTP time server

Note: Date/Time should be set correctly before recording.

4-1. Time synchronization: There are options to choose from.

- Time synchronization can be applied to all connected cameras.
- You can also make this NVR as time server so that the time synchronization can be applied to all the connected devices.
- You can have the time on the system to be synchronized with the NTP time server.



Time

Time zone

(GMT +8:00) Beijing, Perth, Singapore, Hong Kong, Taipei

Current time

1/20/2015 4:15 PM

Time synchronization

☑ Make NVR as time server

□ Apply sync time setting to all added cameras

□ Sync with NTP time server

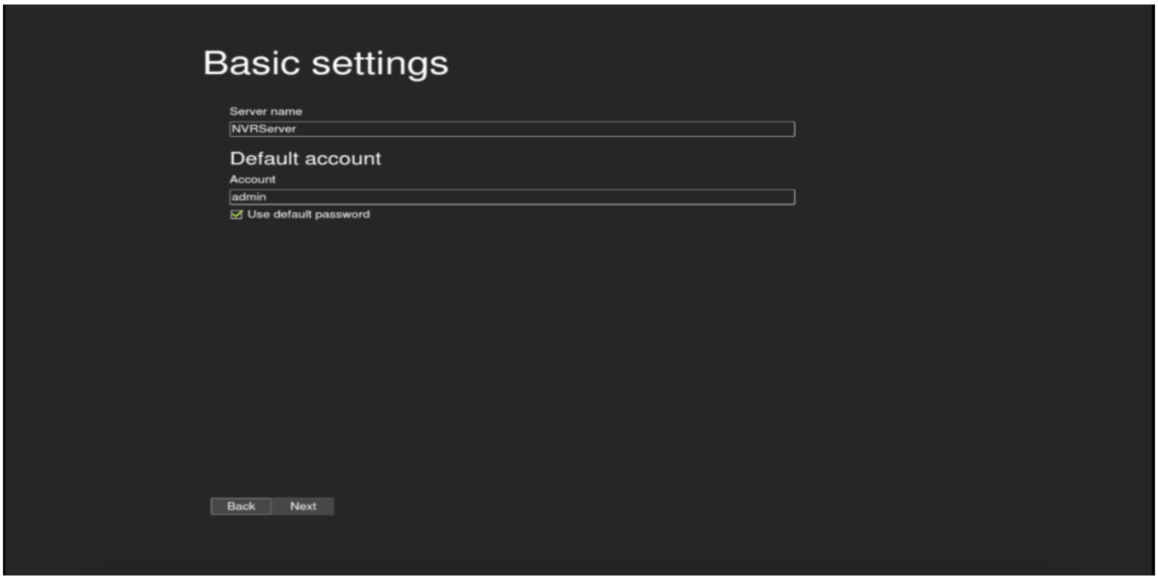
Click **“Next”** to go to the next step **Basic settings**.

5. Basic Settings: You can change or use the default password.

Check the **“Use Default Password”** option, if you wish to keep the default password.

If you want to change the password, input a new password and confirm the newly created password.

Note: The system will restart when the server name is changed.



Basic settings

Server name: NVRServer

Default account

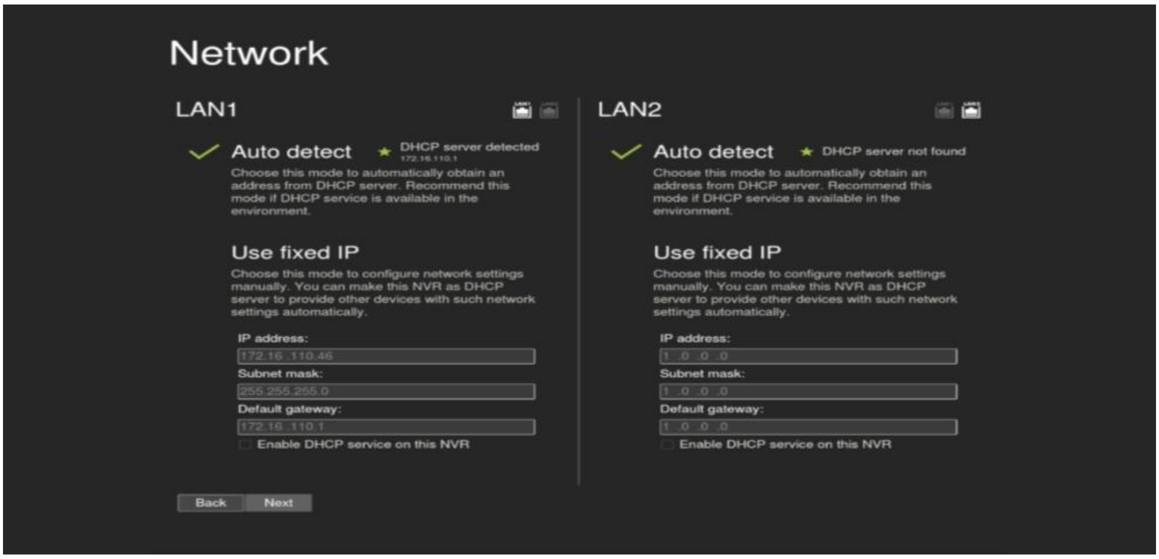
Account: admin

☑ Use default password

Click **“Next”** to go to the next step **Network**.

6. Network: Different network settings can be applied to 2 LANs if there are 2 LANs on the system. It is recommended to select **"Auto detect"** , since the system will detect if there is any DHCP server available. If yes, it will assign an IP address.

You also can select **"Use fixed IP"** to input the IP address of this NVR and make this NVR as a DHCP server. After selecting, input the relevant information and check **"Enable DHCP service on this NVR"** to confirm the setting.



Network

LAN1

✓ Auto detect ★ DHCP server detected 172.16.110.1

Choose this mode to automatically obtain an address from DHCP server. Recommend this mode if DHCP service is available in the environment.

Use fixed IP

Choose this mode to configure network settings manually. You can make this NVR as DHCP server to provide other devices with such network settings automatically.

IP address: 172.16 .110.46

Subnet mask: 255.255.255.0

Default gateway: 172.16 .110.1

□ Enable DHCP service on this NVR

LAN2

✓ Auto detect ★ DHCP server not found

Choose this mode to automatically obtain an address from DHCP server. Recommend this mode if DHCP service is available in the environment.

Use fixed IP

Choose this mode to configure network settings manually. You can make this NVR as DHCP server to provide other devices with such network settings automatically.

IP address: 1 .0 .0 .0

Subnet mask: 1 .0 .0 .0

Default gateway: 1 .0 .0 .0

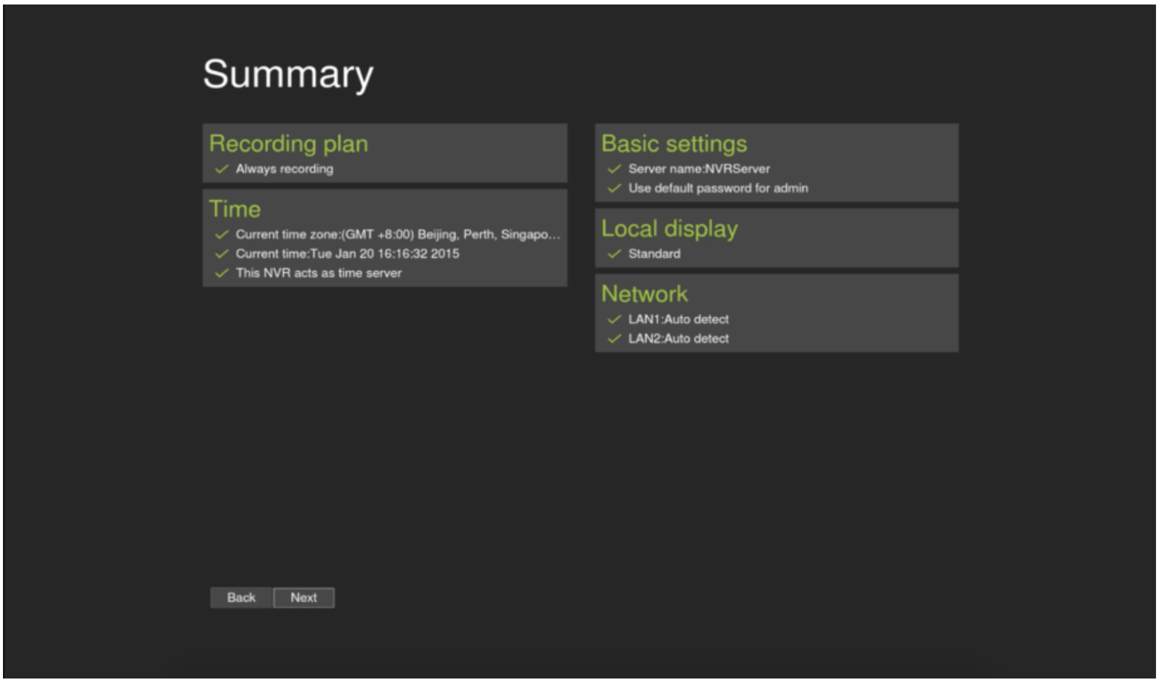
□ Enable DHCP service on this NVR

Warning: Make sure that only 1 DHCP server is activated in your system, otherwise it may cause network errors.

Note: You can also change the network settings, once you're logged in to the Local Client. Go to *Setup* > *Network* > *DHCP Server* for the network configuration.

Click **"Next"** to go to the next step **Summary**.

7. Summary: This page shows the setting results you have set so far. Check if the results are what you wished for. If not, click on the items to go back the items you wish to modify and set up again.



Summary

Recording plan

✓ Always recording

Time

✓ Current time zone:(GMT +8:00) Beijing, Perth, Singapo...
✓ Current time:Tue Jan 20 16:16:32 2015
✓ This NVR acts as time server

Basic settings

✓ Server name:NVRServer
✓ Use default password for admin

Local display

✓ Standard

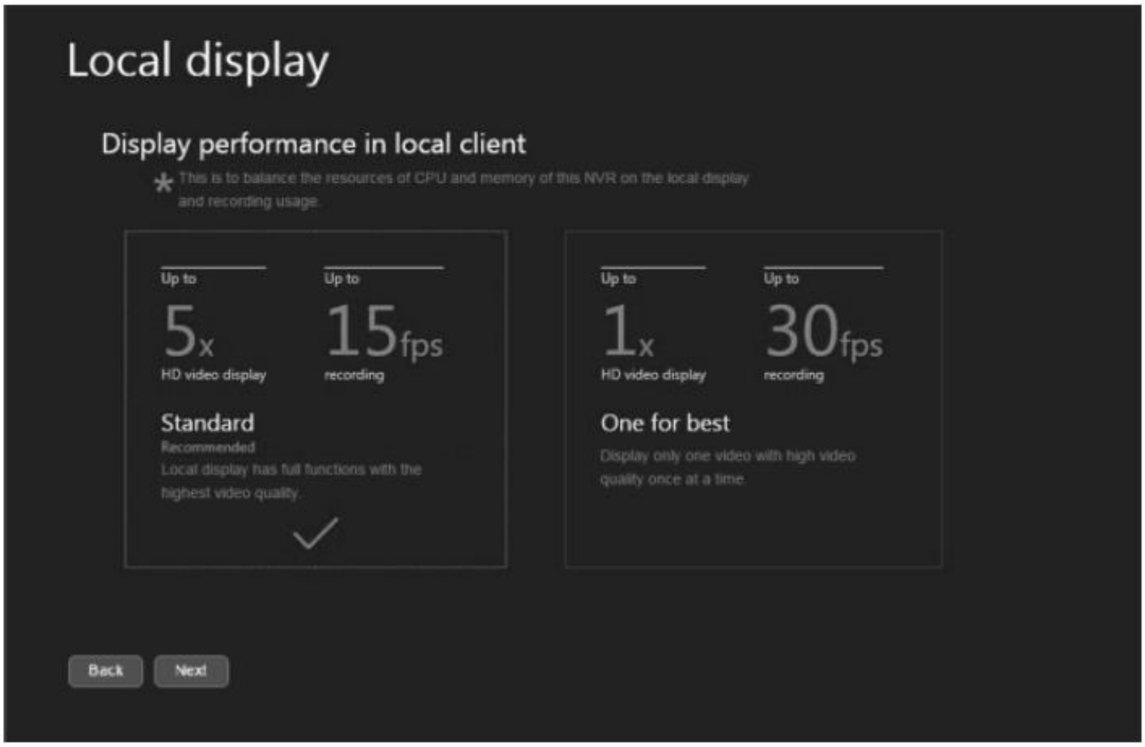
Network

✓ LAN1:Auto detect
✓ LAN2:Auto detect

After clicking “**Next**”, the wizard will start to initialize your system and go to the next step **Progressing**.

If you wish to set up the local display, you can click this item and go to the Local display page.

Local display: Select the best method for your scenario to have a balanced resource usage for the quality of recording and local display.



Local display

Display performance in local client

* This is to balance the resources of CPU and memory of this NVR on the local display and recording usage.

Up to 5x HD video display

Up to 15fps recording

Standard

Recommended

Local display has full functions with the highest video quality.

✓

Up to 1x HD video display

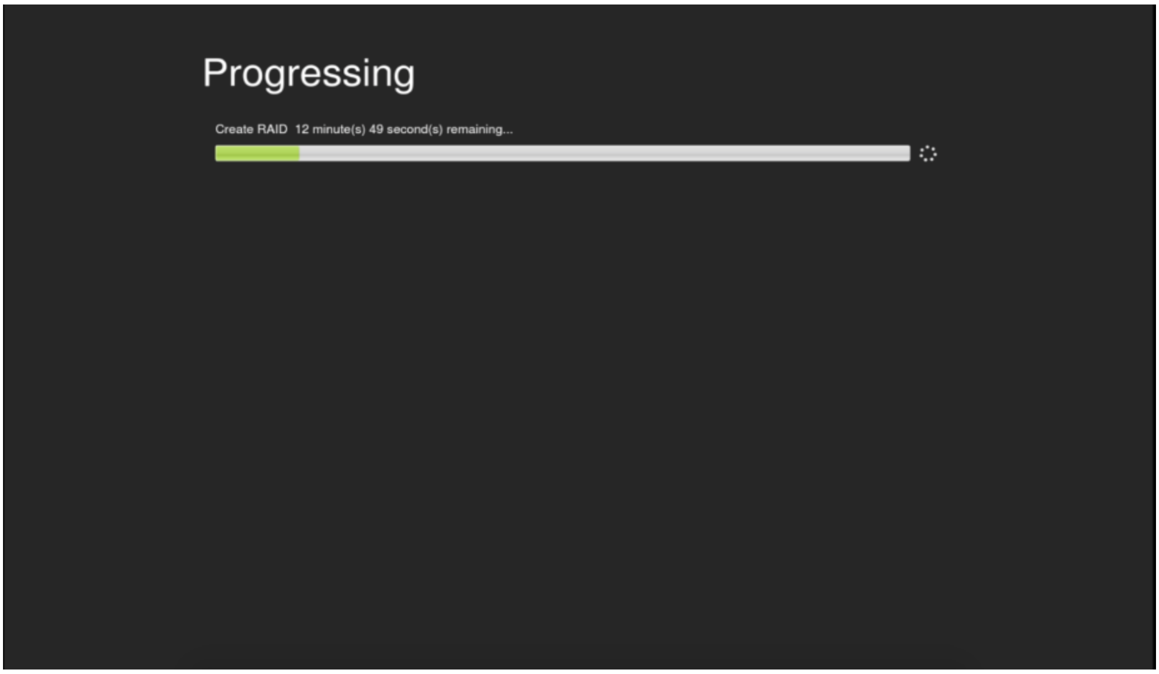
Up to 30fps recording

One for best

Display only one video with high video quality once at a time.

Note: The system will restart when the setting is changed.

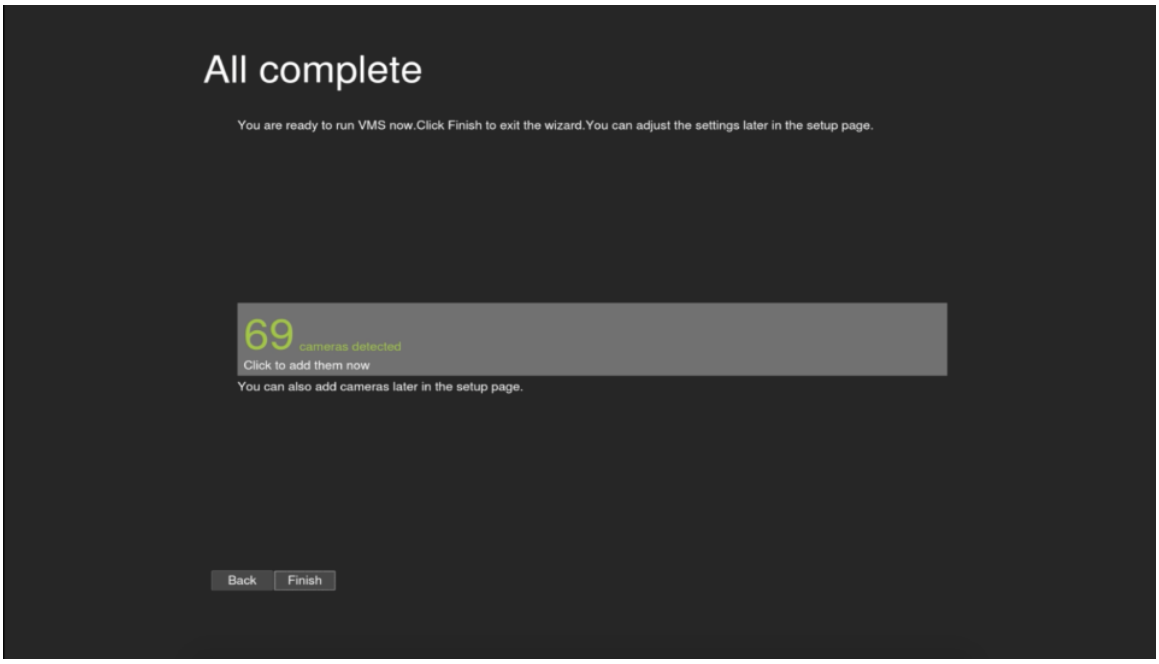
8. **Progressing**: After clicking “Next” on the summary page, the wizard will start to initialize your system. This act will take a few minutes to complete. Once it is done, the system will reboot automatically.



Progressing

Create RAID 12 minute(s) 49 second(s) remaining...

9. All complete: All the necessary settings are done. Click “Finish” to close this window and the system will be directed to the VMS. You can modify and configure more settings later in the setup page.



All complete

You are ready to run VMS now.Click Finish to exit the wizard.You can adjust the settings later in the setup page.

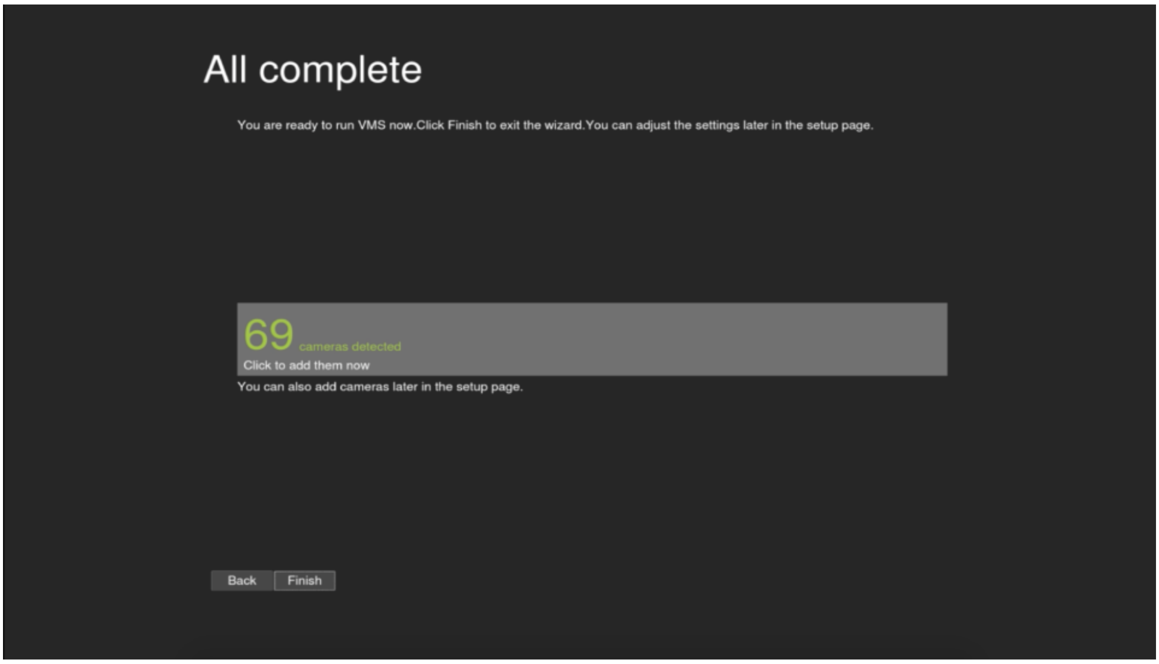
69 cameras detected

Click to add them now

You can also add cameras later in the setup page.

9-1. **Camera detection**: The system will detect the cameras in the same LAN. Click the **detection result** to go to the next step **Add camera**.

Click “**Finish**” to close this window. You can add cameras later in the setup page.



All complete

You are ready to run VMS now.Click Finish to exit the wizard.You can adjust the settings later in the setup page.

69 cameras detected

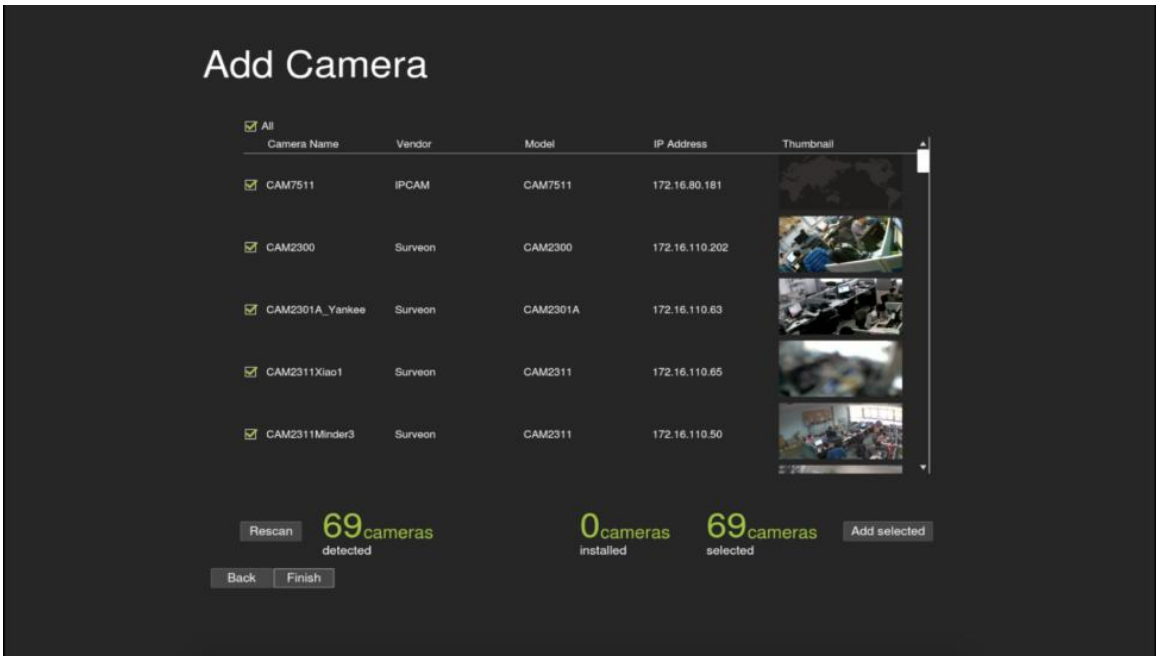
Click to add them now

You can also add cameras later in the setup page.

10. **Add camera:** The detected cameras will be shown here. Select the cameras you wish to add and click “**Add selected”** to add the selected cameras.

Click “**Rescan”** to detect the cameras again.

Click “**Finish**” to close this window. You can also add cameras later in the setup page.



Add Camera

☑ All

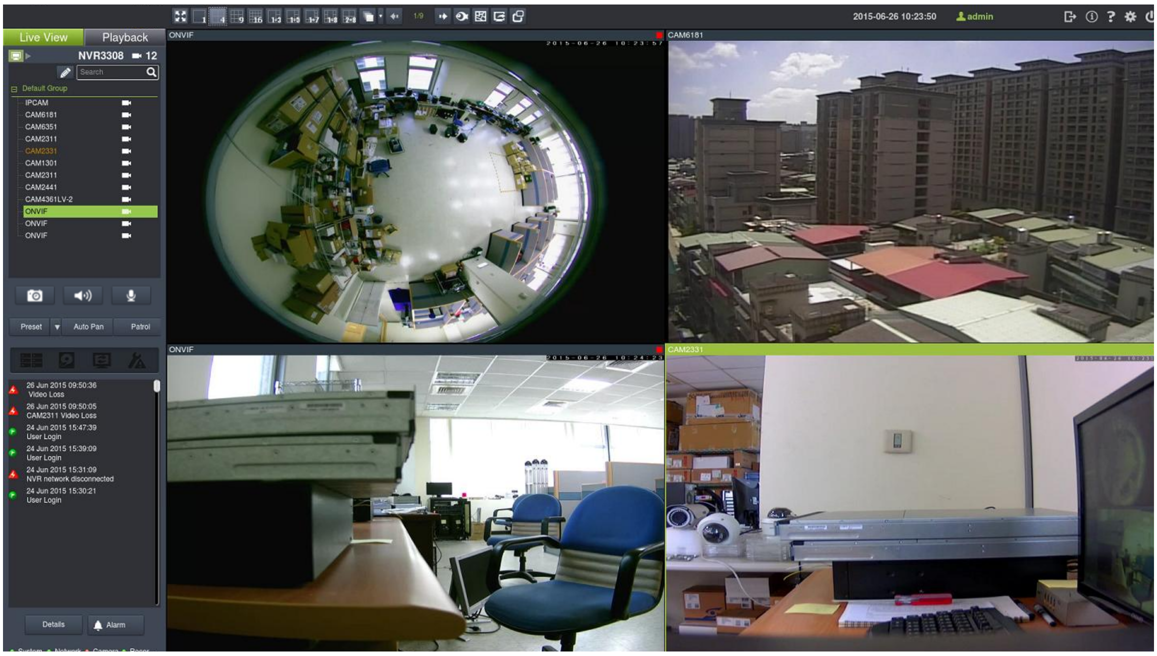
	Camera Name	Vendor	Model	IP Address	Thumbnail
☑	CAM7511	IPCAM	CAM7511	172.16.80.181	
☑	CAM2300	Surveon	CAM2300	172.16.110.202	
☑	CAM2301A_Yankee	Surveon	CAM2301A	172.16.110.63	
☑	CAM2311Xiao1	Surveon	CAM2311	172.16.110.65	
☑	CAM2311Minder3	Surveon	CAM2311	172.16.110.50	

69 cameras detected

0 cameras installed

69 cameras selected

After the wizard installation is done, you will see the **Live View** page from the **Local Client**.



26 Jun 2015 09:50:36
Video Loss

26 Jun 2015 09:50:05
CAM2311 Video Loss

24 Jun 2015 15:47:39
User Login

24 Jun 2015 15:39:09
User Login

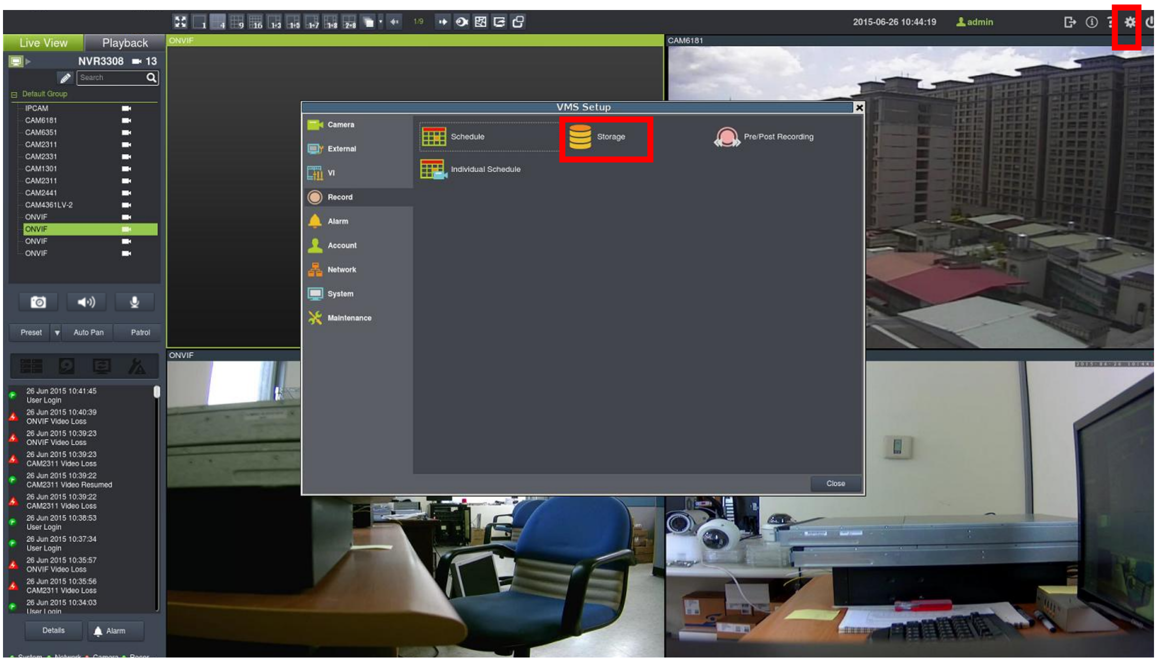
24 Jun 2015 15:31:09
NVR network disconnected

24 Jun 2015 15:30:21
User Login

Chapter 5. Basic System Settings

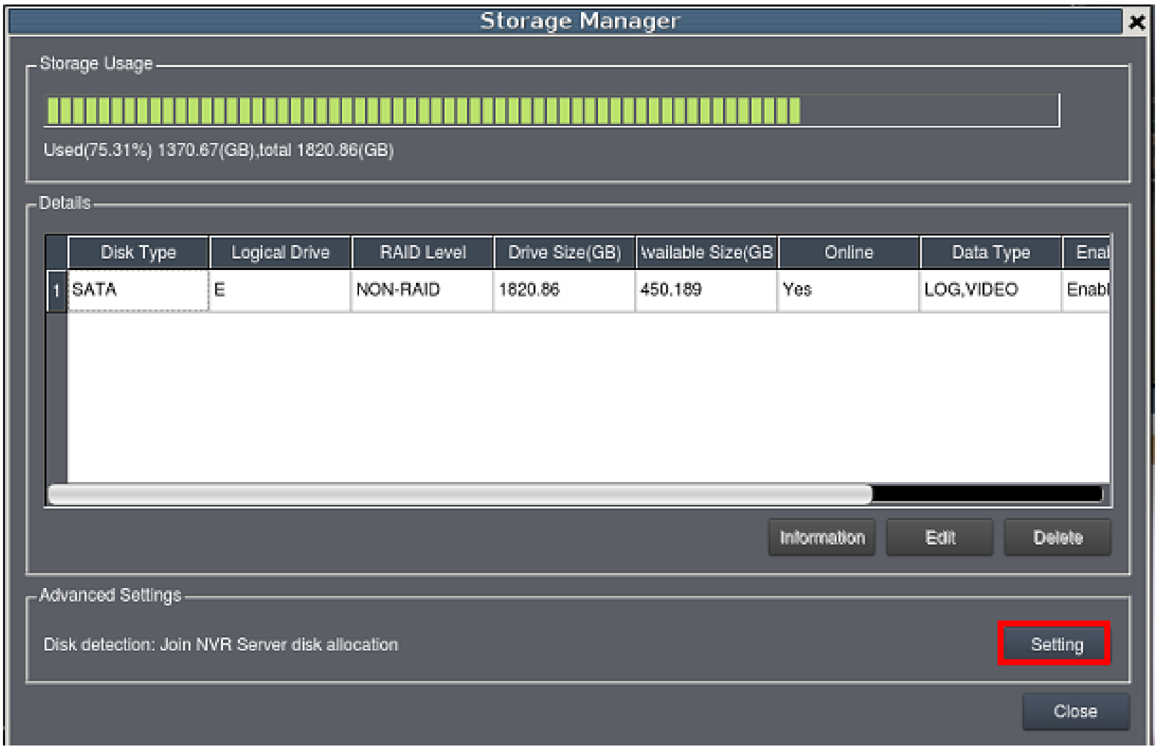
5.1. Storage Management

1. To access the information about the drives configured in your Server, click **Setup** to bring out **VMS Setup** window and then select **Recording** to see and click **Storage** option for **Storage Manager**.



```
26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
```

2. All available Logical Drives, as well as their sizes, free space, and status will appear. Click target drive and then **Setting** to set the log and location for saving the video recordings.



Storage Manager

Storage Usage

Used(75.31%) 1370.67(GB),total 1820.86(GB)

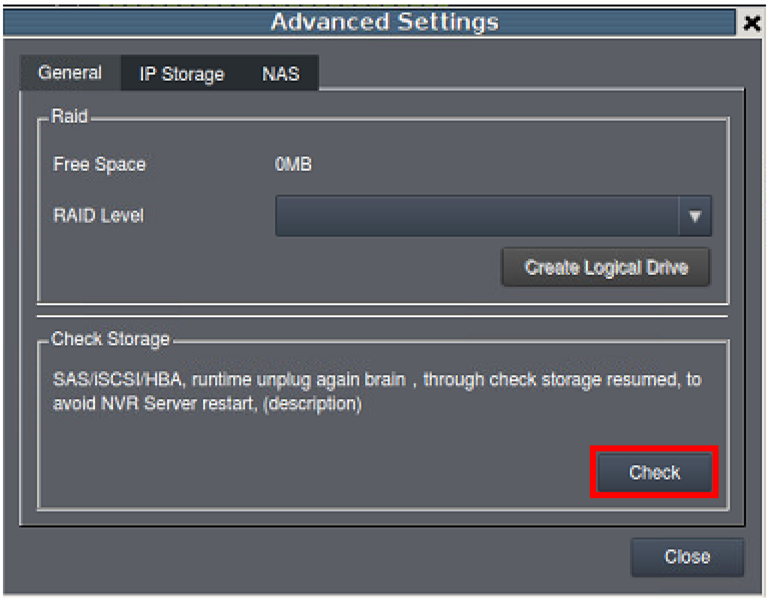
Details

	Disk Type	Logical Drive	RAID Level	Drive Size(GB)	Available Size(GB	Online	Data Type	Enal
1	SATA	E	NON-RAID	1820.86	450.189	Yes	LOG,VIDEO	Enabl

Advanced Settings

Disk detection: Join NVR Server disk allocation

3. Click the target drive first and then **Settings**. In “General” tab, click **Check**.



Advanced Settings

Raid

Free Space 0MB

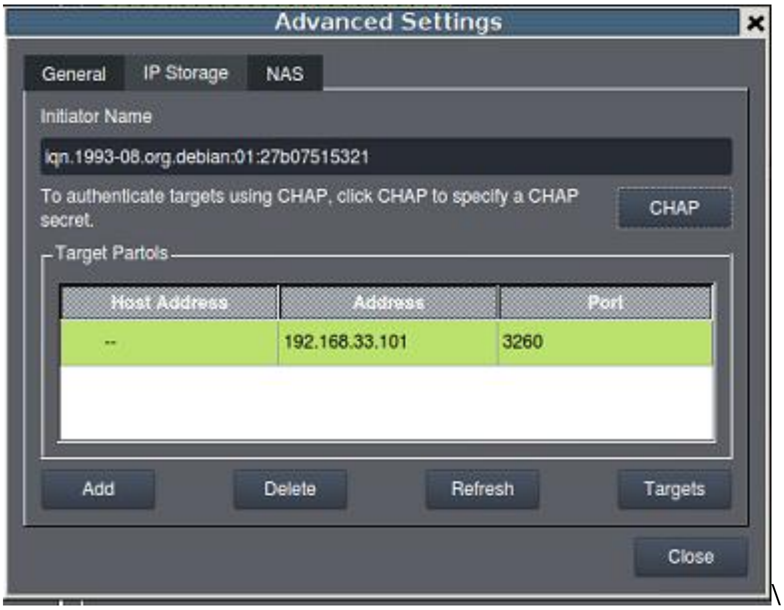
RAID Level

Check Storage

SAS/ISCSI/HBA, runtime unplug again brain , through check storage resumed, to avoid NVR Server restart, (description)

4. Choose the RAID level, and then click **Create Logical Drive** to create the RAID configuration. The system supports recording to ISCSI and NAS.

5. In “IP Storage” tab, you can authenticate targets by clicking CHAP to setup CHAP.



Initiator Name

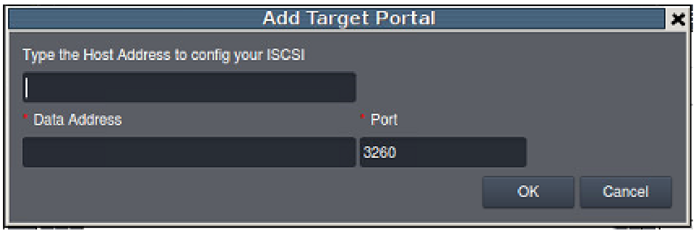
iqn.1993-08.org.debian:01:27b07515321

To authenticate targets using CHAP, click CHAP to specify a CHAP secret.

Target Partols

Host Address	Address	Port
--	192.168.33.101	3260

- Add: Clicking Add and input the required information to add more targets.



Type the Host Address to config your ISCSI

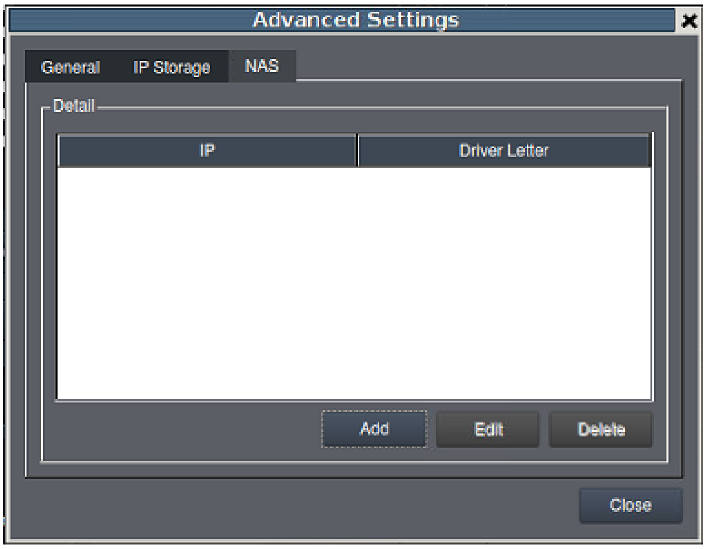
* Data Address

* Port

3260

- Delete: Clicking Delete to delete the selected.
- Refresh: Clicking Refresh to refresh.
- Target: Click Targets to see the setup result.

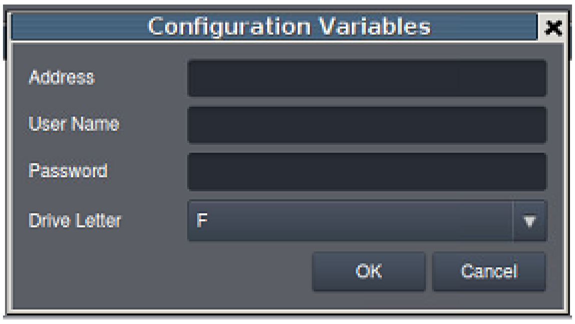
6. In “NAS” tab, you can add NAS in as the video storage.



Detail

IP	Driver Letter

Clicking Add and input the required information to add NAS as the video storage.



Configuration Variables

Address

User Name

Password

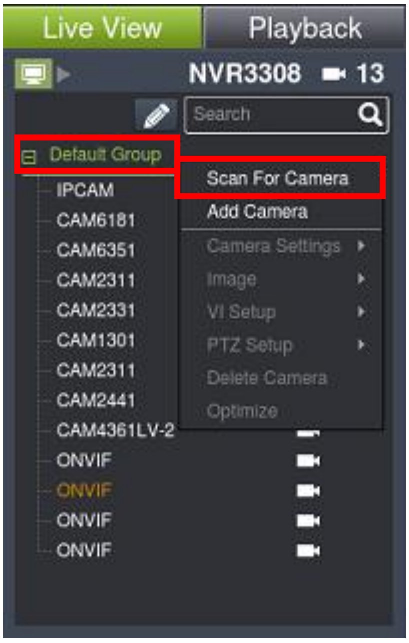
Drive Letter F

5.2. Adding Cameras to the Server

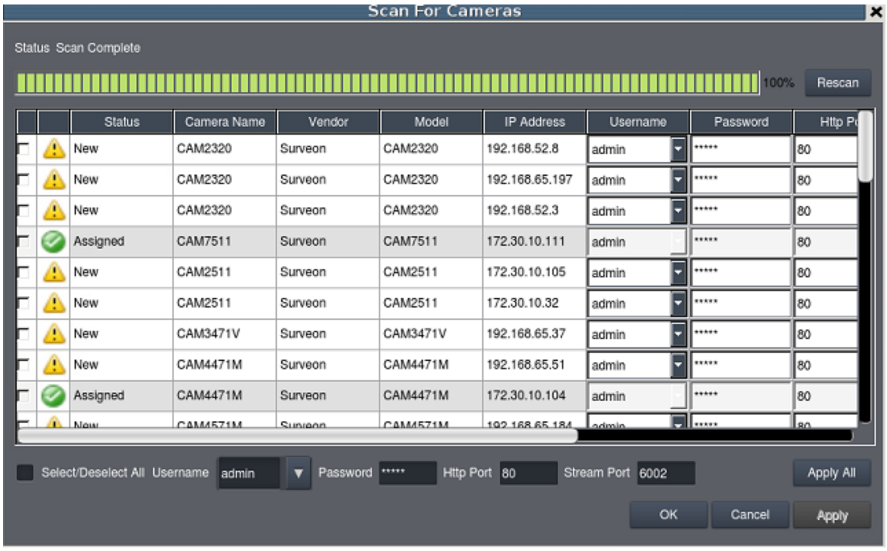
Cameras can be added to the Server in two ways: via an automatic scan or by manually inputting the camera information.

5.2.1. Automatic Scan for Cameras

Right-click on the “Default Group” area to bring out the setting menu and select **Scan For Camera**.



1. The system will respond by beginning an automatic scan. Once the scan is complete, the cameras that can be added to the Server will be displayed. Information available for each camera will include:



Status Scan Complete

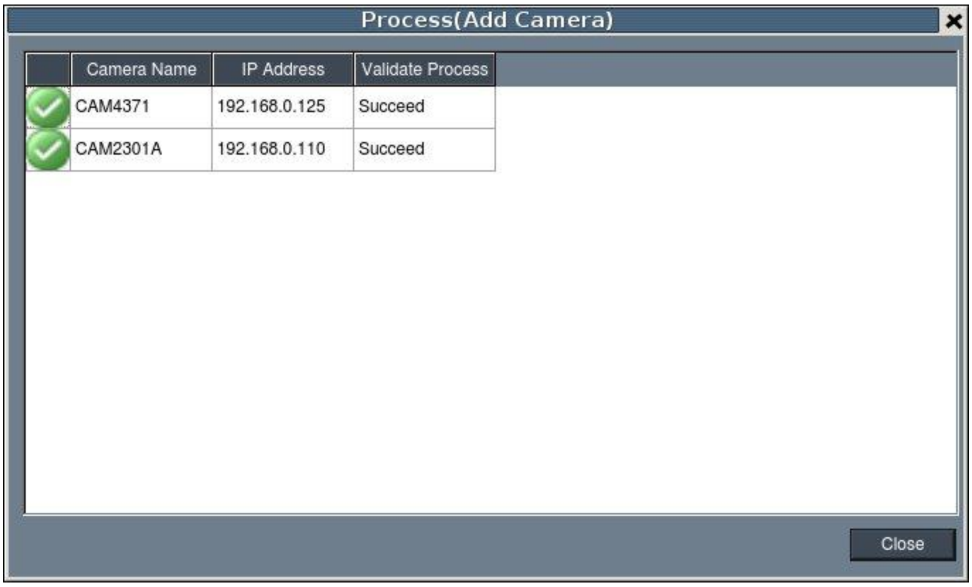
		Status	Camera Name	Vendor	Model	IP Address	Username	Password	Http P
□	⚠	New	CAM2320	Surveon	CAM2320	192.168.52.8	admin	*****	80
□	⚠	New	CAM2320	Surveon	CAM2320	192.168.65.197	admin	*****	80
□	⚠	New	CAM2320	Surveon	CAM2320	192.168.52.3	admin	*****	80
□	✓	Assigned	CAM7511	Surveon	CAM7511	172.30.10.111	admin	*****	80
□	⚠	New	CAM2511	Surveon	CAM2511	172.30.10.105	admin	*****	80
□	⚠	New	CAM2511	Surveon	CAM2511	172.30.10.32	admin	*****	80
□	⚠	New	CAM3471V	Surveon	CAM3471V	192.168.65.37	admin	*****	80
□	⚠	New	CAM4471M	Surveon	CAM4471M	192.168.65.51	admin	*****	80
□	✓	Assigned	CAM4471M	Surveon	CAM4471M	172.30.10.104	admin	*****	80
□	⚠	New	CAM4571M	Surveon	CAM4571M	192.168.65.184	admin	*****	80

□ Select/Deselect All Username admin ▼ Password ***** Http Port 80 Stream Port 6002

- **Name** – The default camera name (Make/Model)
- **Status** – The camera will display *New* if it has not been added to this Server, otherwise it will display *Assigned*.
- **IP Address**
- **MAC Address**
- **Vendor - Including ACTI, Afreey, AXIS, Arecont, BOSCH, Dahua, Dynacolor, EDIMAX, EverFocus, HIKVISION, IQinvision, JVC, LG, Panasonic, Surveon, and ONVIF.**
- **Model**

2. To add a camera to the system, check the box by the camera entry. You may also check the **Select All** box at the bottom of the window to select all the cameras found.
   Enter the username and password, and press **Apply Selected**. Click **OK** to add the selected cameras to the Server.

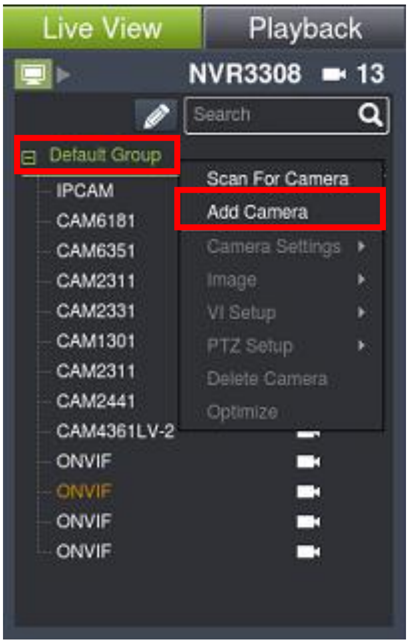
The following windows will prompt for validation.



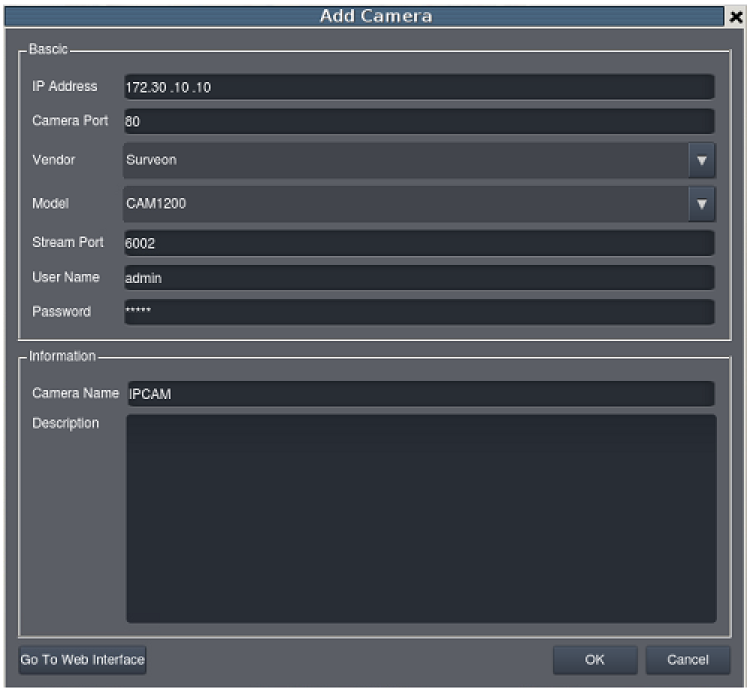
	Camera Name	IP Address	Validate Process
✓	CAM4371	192.168.0.125	Succeed
✓	CAM2301A	192.168.0.110	Succeed

5.2.2. Manually Adding Cameras

Right-click on the “Default Group” area to bring out the setting menu and select **Add Camera** to manually add a camera to the Server.



2. In the camera window fill out the following information:


Add Camera

Basic

IP Address	172.30 .10 .10
Camera Port	80
Vendor	Surveon
Model	CAM1200
Stream Port	6002
User Name	admin
Password	*****

Information

Camera Name	IPCAM
Description	

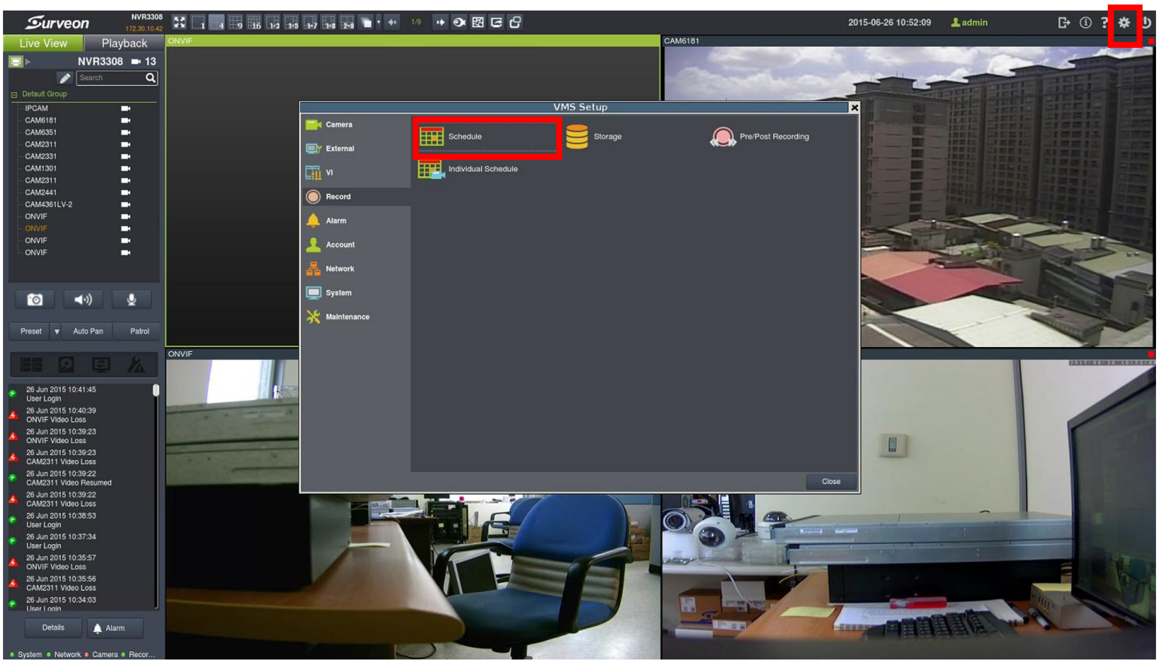
- **IP Address**
- **Camera Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.

- **Vendor - Including Including ACTI, Afreey, AXIS, Arecont, BOSCH, Dahua, Dynacolor, EDIMAX, EverFocus, HIKVISION, IQinvision, JVC, LG, Panasonic, Surveon, and ONVIF.**
- **Stream Port -** This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

5.3. Setting Recording Schedule

5.3.1. Recording Schedule

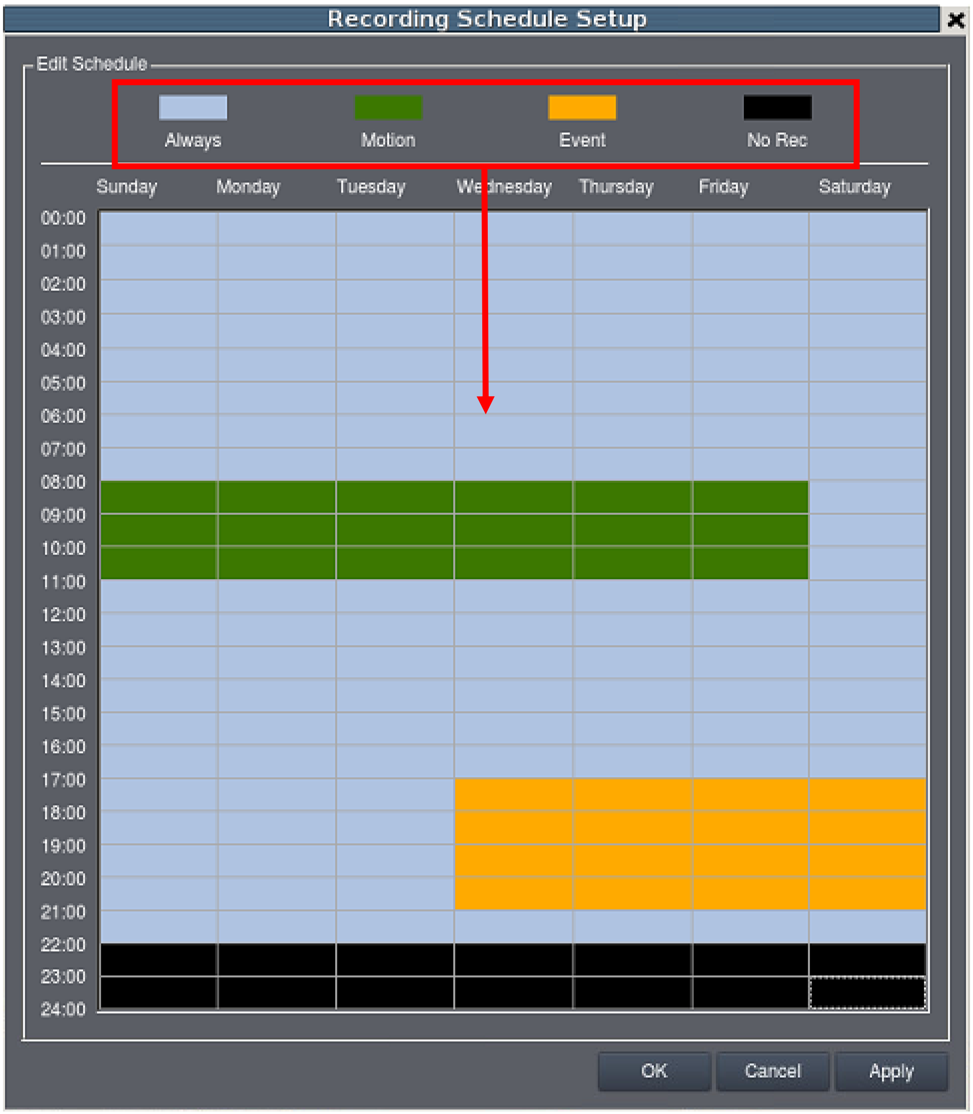
Click ⚙ to bring out **VMS Setup** window and select **Record** and then **Schedule**.



26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login

1. The schedule grid corresponds to every hour in the week. Click on one of the 4 recording methods and then click on the grid area to “paint in” the method for the corresponding hour.

2. Click the **Apply** button to apply the schedule and **OK** to exit the dialog.



🟦 Always 🟩 Motion 🟧 Event ⬛ No Rec

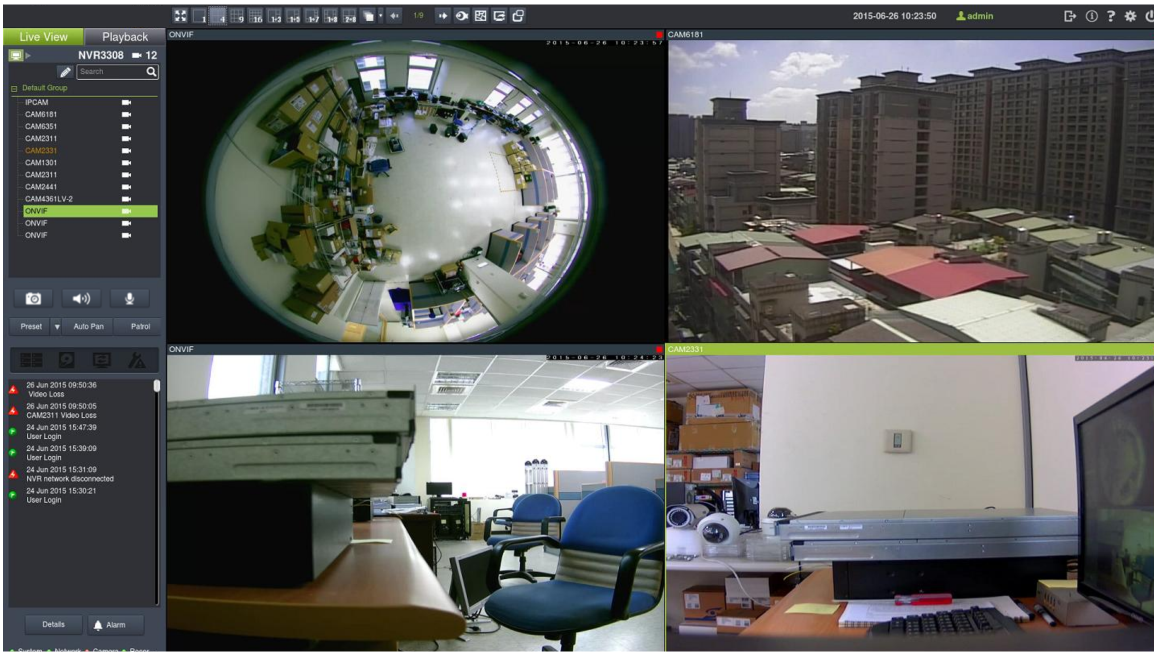
	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
01:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
02:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
03:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
04:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
05:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
06:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
07:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
08:00	🟩	🟩	🟩	🟩	🟩	🟩	🟦
09:00	🟩	🟩	🟩	🟩	🟩	🟩	🟦
10:00	🟩	🟩	🟩	🟩	🟩	🟩	🟦
11:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
12:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
13:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
14:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
15:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
16:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
17:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
18:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
19:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
20:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
21:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
22:00	⬛	⬛	⬛	⬛	⬛	⬛	⬛
23:00	⬛	⬛	⬛	⬛	⬛	⬛	⬛
24:00							

5.4. Setting up Live View

An important part of monitoring your surveillance network is to have the right views so that you will have the optimum viewing angle to discern a situation.

The default view setting is 4x4.

From the *Camera List*, you can click and drag each camera into separate frames. The camera output will be displayed in the frame.



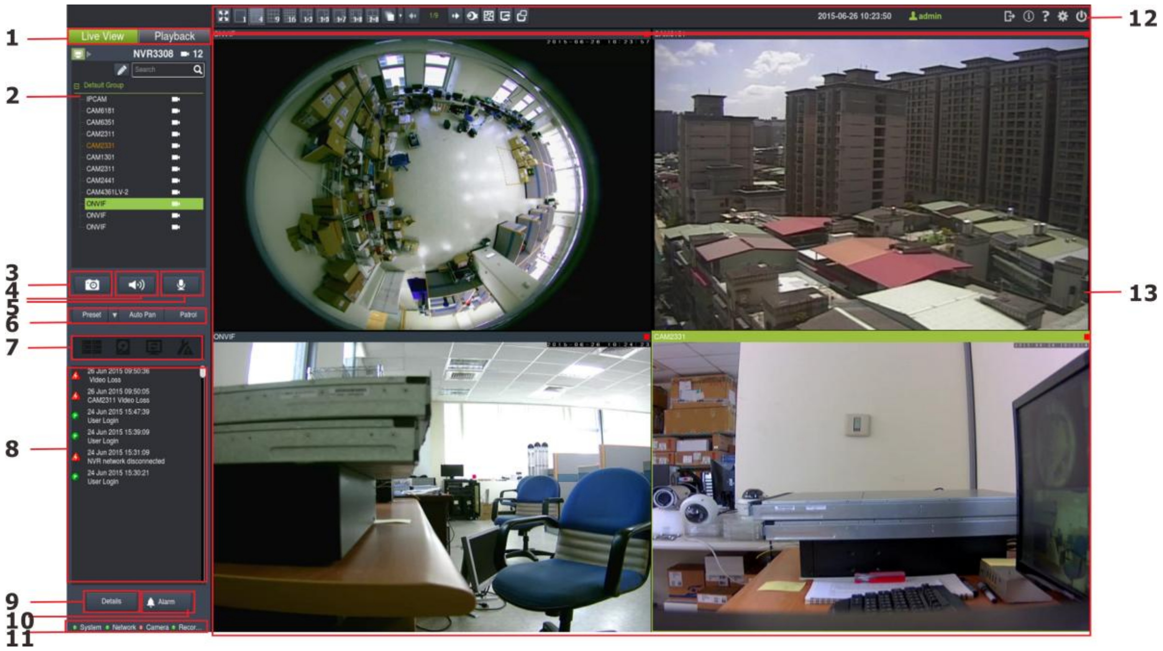
26 Jun 2015 09:50:36
Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected
24 Jun 2015 15:30:21
User Login

Chapter 6 Live View

Live viewing is a crucial part of any surveillance system. Having the right view can be the crucial difference between catching an event as it happens and missing it altogether. VMS provides powerful tools to manage the viewing experience to help ensure that monitoring personnel are always on top of any event.

6.1. Live View Window Overview

The live view window is split into 10 distinct parts:



1. **Live View / Playback Selection Tabs** – Allows users to choose live view and playback mode.

2. **Camera List** – Lists all the connected cameras.

3. **Snapshot** – Take a snapshot of the current camera image.

4. **Volume Control** – Control the volume.

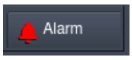
5. **Microphone** – Enable/Disable the microphone functionality.

6. **Live View Control** – PTZ functions, including Preset, Auto Pan, and Patrol for PTZ-enabled cameras.

7. **System Health Diagnosis** – Displays RAID problems, disk failure, service problems, fan/power failures.

8. **Log** - This area contains all the logs. system, video, storage, network status information.

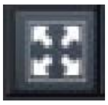
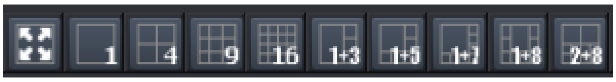
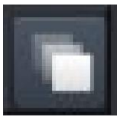
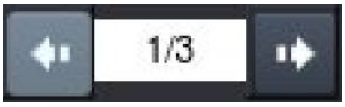
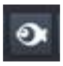
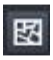
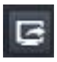
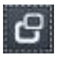
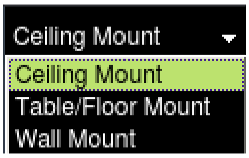
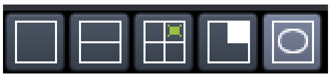
9. **Details** – List all the detailed logs for review, query and export.

10. **Alarm** – When triggered, the icon will flick with a red colored alarm 

.

11. **System status** - This area contains system, network, camera, recording status information.

12. **Button Area** - This area contains the buttons to change views, enter the full screen mode, go to the next/previous page, go home and auto page flip between pages.

	Full screen mode
	Viewing screen modes
	Auto page flip between pages
	When there are more than 1 live view page, click these buttons to go to the next / previous page.
	Select this icon to have better views for fisheye camera
	E-map
	Send to the Secondary Display
	PAP View
 Ceiling Mount Ceiling Mount Table/Floor Mount Wall Mount	Select according to the way your fisheye is installed to have a best viewing result, Ceiling Mount, Table/Floor Mount or Wall Mount.
	The distorted hemispherical image of the fisheye camera can be converted into a

	conventional rectilinear projection ▢, a split-window ⊟, a 4 split-window ⊞ with 3 enlarge windows and 1 original image window, ◲ an enlarged window and the original fisheye view ◯.
2015-06-26 13:13:26	Date and time
👤admin	Signed in User Account
⇥	Logout
ⓘ	About contains version and product information
?	Enclosed with the user manual
⚙	Setup button
⏻	Shutdown button

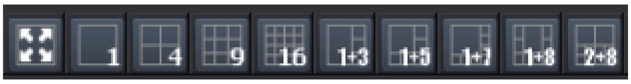
13. **Main View Area** – This area contains the actual video feed(s).

6.2. View Setup

6.2.1. Switching Between Different Screen Divisions

Creating and Using New Screen Divisions

When a view is created, it has a default screen division setting, however when using the view, it may be useful to change the number of screen divisions. This does not create a different view, but divides the existing view into a new set of divisions.

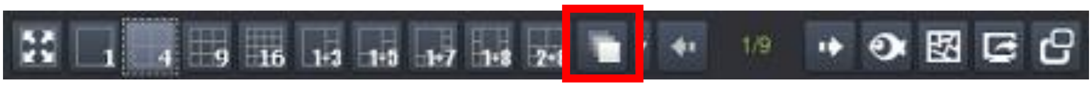


To perform this function within the view, simply click the button corresponding to the view that you want to use. The buttons are located in the area above the main view window.

After you have clicked on the desired view, the cameras will be divided into separate pages in the selected view; the formula is 36/selected view number. For example, a one view will have a 36 pages of views and a 1+5 view will be 36/6, 6 pages of views.

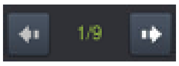
Auto-flipping Pages

When multiple pages of screen divisions exist, you may choose to automatically flip between the pages by clicking on the button. Clicking the button again will end the automatic flip function.



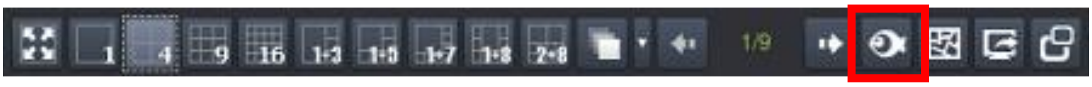
Screen Division Page Use

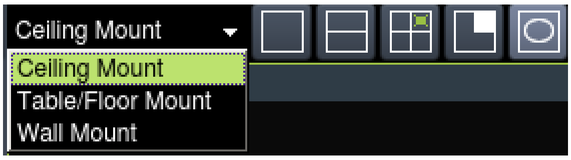
The page number is displayed to the right of the view buttons. Clicking on the arrow button to the right of the page number or clicking on the current screen partition button will scroll through the pages in order. Clicking on the arrow button to the left of the page number will scroll through the pages in reverse order.



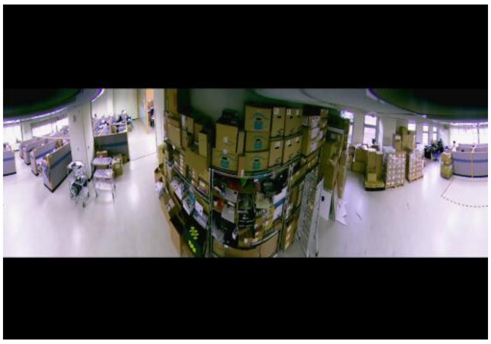
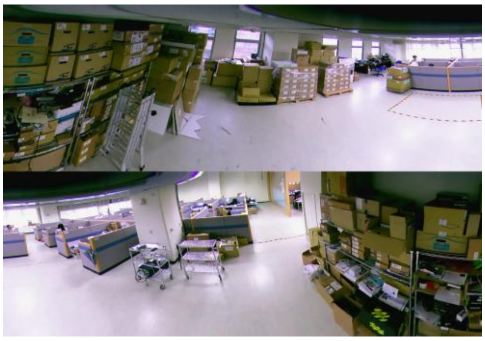
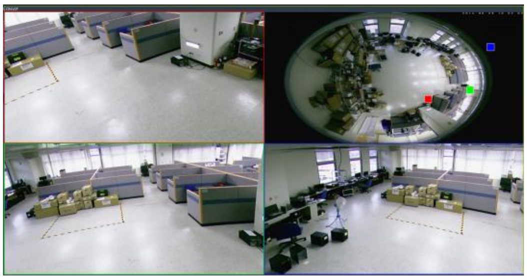
Fisheye View

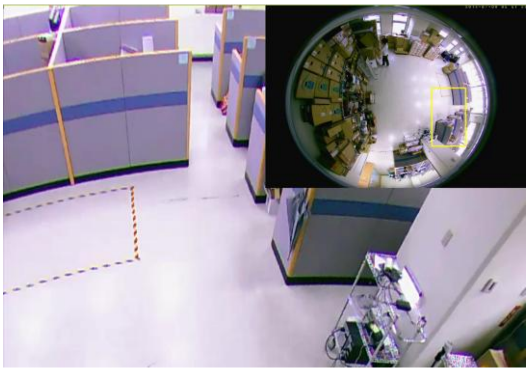
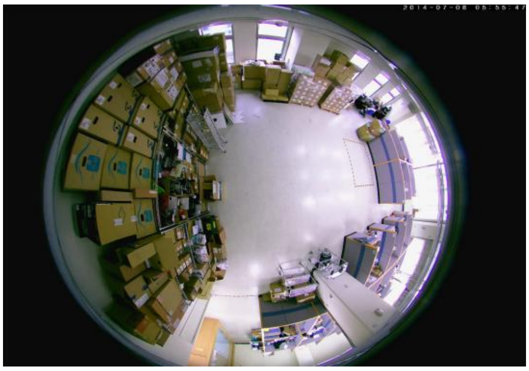
Click the **Fisheye** button in the button area when using a fisheye camera. This will bring out a selection of views for fisheye camera to have better view results.





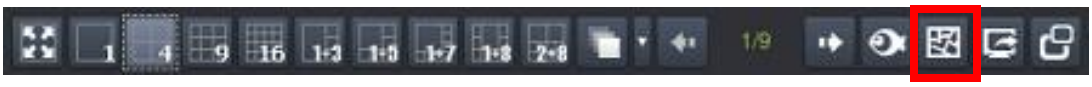
Select according to the way your fisheye is installed to have a best viewing result, Ceiling Mount, Table/Floor Mount or Wall Mount.

Icon	Description	Reference
□	conventional rectilinear projection, panorama view	
⊟	split-window, horizontal view	
⊞	4 split-windows: 3 enlarged view windows and 1 original fisheye window. Place the different colored boxes in the original fisheye window on the upper right corner to have detailed views projected on the other viewing windows.	

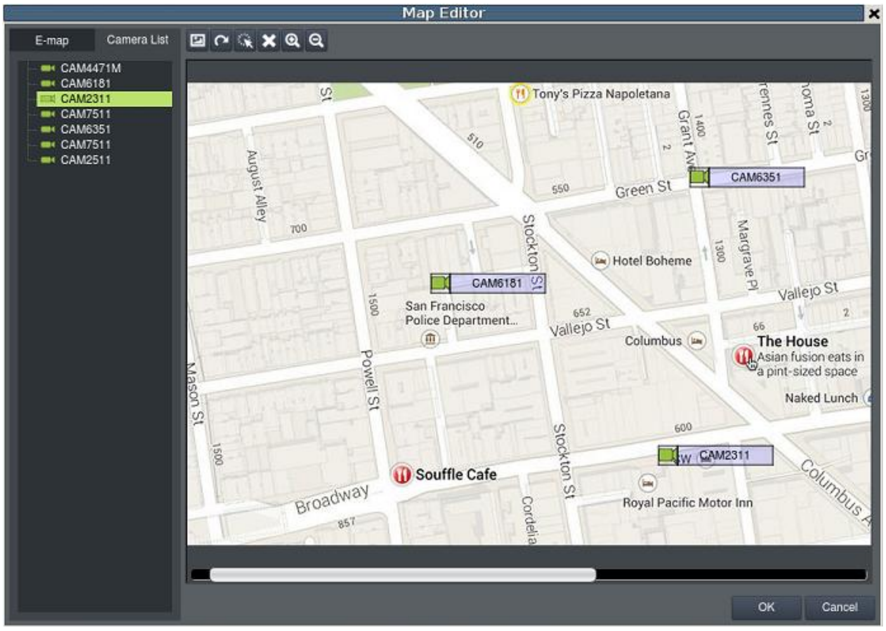
◰	1 enlarged view window and 1 an original fisheye window. Place the colored box in the original fisheye window on the upper right corner to have a detailed view projected.	
○	original fisheye view	

E-map

Click the **E-map** button in the button area to open an existing E-map or create an E-map.

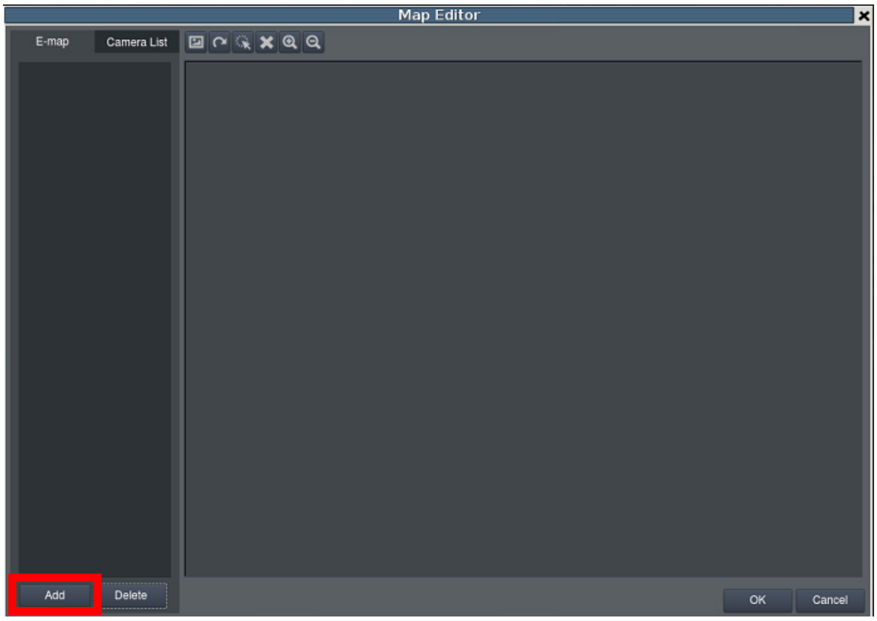


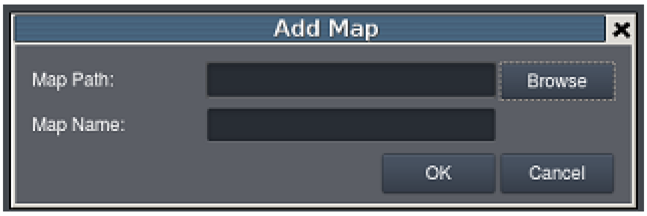
When there is an existing E-map, the E-map will be shown as below. You can click the set camera on the map to see its surroundings. If there is an alarm, the set camera on the E-map will begin flicking and you can have a better idea where the event took place.



When there is no E-map stored, the system will ask you to add an E-map. Follow the steps below to create an E-map.

1. Prepare layout drawings or a map of the area being surveyed.
2. Click the **Add** button to bring out the **Add Map** window.



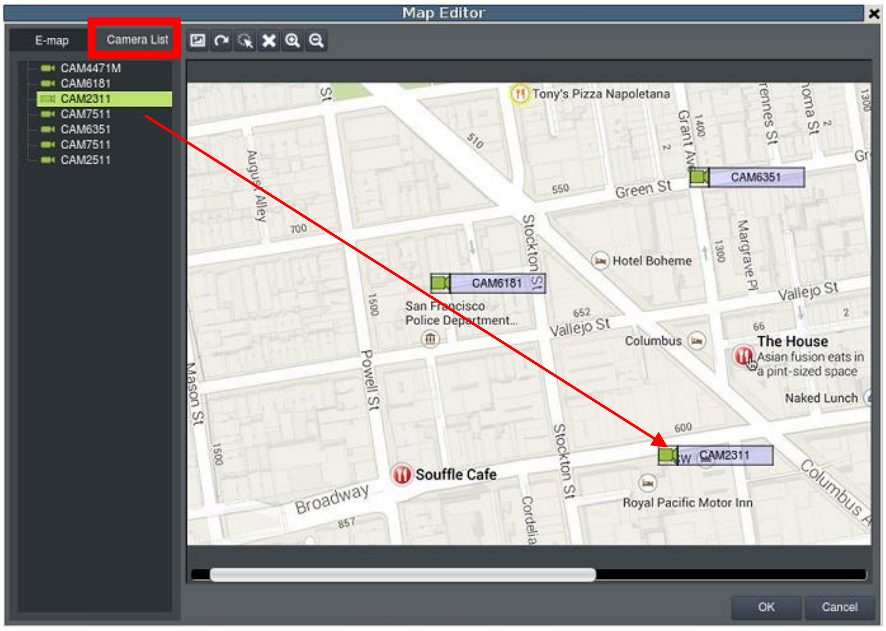


3. Click the **Browse** button to open a windows dialog. Select your map and click the **Open** button. The drawing will be stored in the Server.

4. Enter a name for the map in the **Map Name** field.

5. Click **Save**. Once successfully added, an E-map node will appear.

6. Go to the Camera List tab to drag and drop the cameras to the desired location on the E-map to complete the E-map creation.



For camera relocation, click to select the cameras and then the selected camera can be moved.

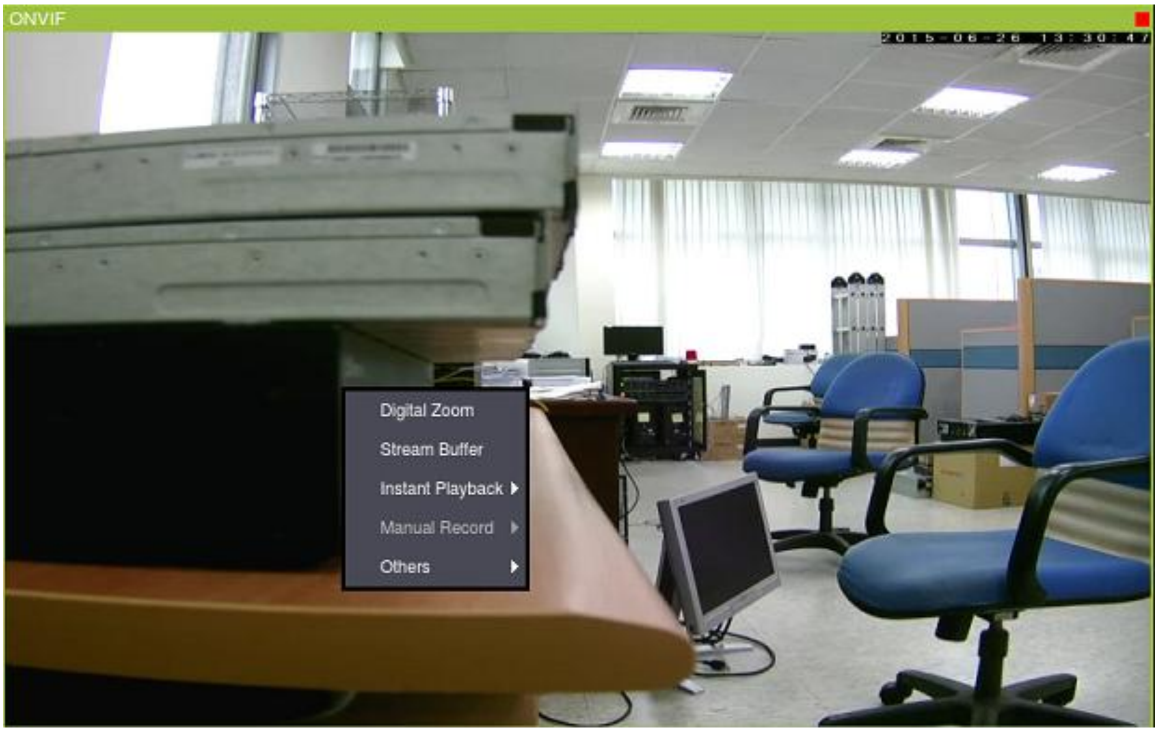
Go to ***VMS Setup*** > ***System*** > ***Map Editor*** in the setup to add another E-map or any further setups.

Secondary Display

Click the **Secondary Display** button in the button area when you have the second monitor, the view will be sent to the secondary display.

6.3. Functionality Within Views

Right clicking an active window will cause a function list to appear. These are settings and functions that can be changed within the live-view window.



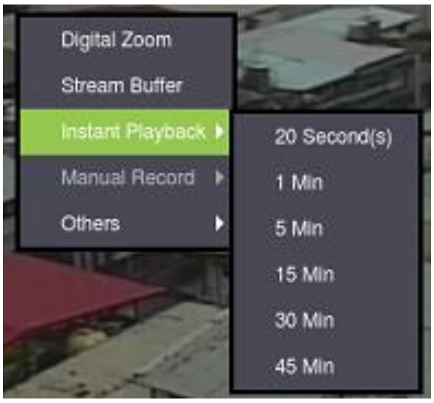
6.3.1. Digital Zoom

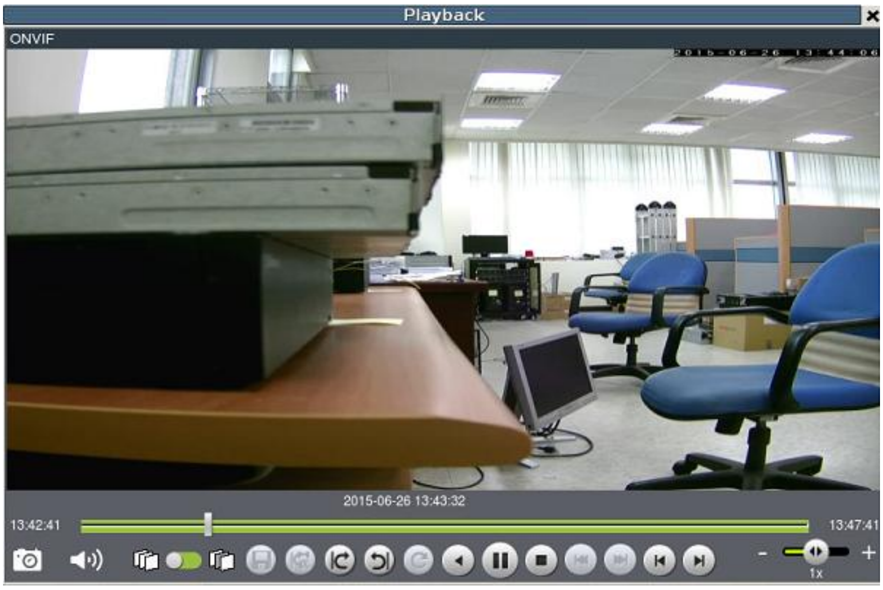
Digital zoom increases the view size without increasing resolution. The digital zoom function can be used within any panel (even in full screen mode) with the following steps:

1. Right-click the panel that zoom is required on, and select **Digital Zoom** to activate the function. A picture-in-picture showing the whole screen framed by a yellow box will appear.
2. Use the mouse scroll to zoom into the center of the image. Scrolling forward will zoom in, scrolling backward will zoom out. Click the corners of the box and drag to the area of interest. The main picture will show the digitally-zoomed output, while the picture and picture will display the entire view.

6.3.2. Instant Playback

The instant playback function gives users the ability to instantly playback up to 45 minutes of video. Right-click the video panel that playback is required on, and select **Instant Play > [Time Length]** to activate the function. A popup will open with the desired playback. Time lengths available are dependent on, and will not exceed the pre-alarm recording time set in Pre/Post Recording .





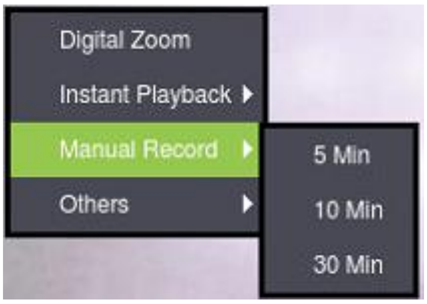
The following table explains the buttons:

📷	Snapshot
🔊	Audio volume
- + 60 Min	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
💾	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start
	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
◀	Play backwards
▶	Starts video playback

⏸	Pause video playback
⏹	Stops video playback.
⏮	Jumps to the previous frame
⏭	Jumps to the next frame
⏮	Jumps to the previous segment
⏭	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

6.3.3. Manual Recording

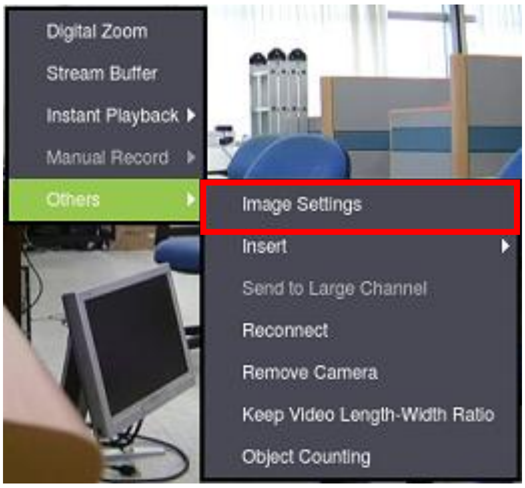
When recording schedules are set, it may be necessary to manually record a video stream, even when the schedule does not specify for recording. In this case right-click the panel that recording is required on, and select **Manual Record > [5, 10 or 30 minutes]** to activate the function. The camera will record the stream for the amount of time specified.

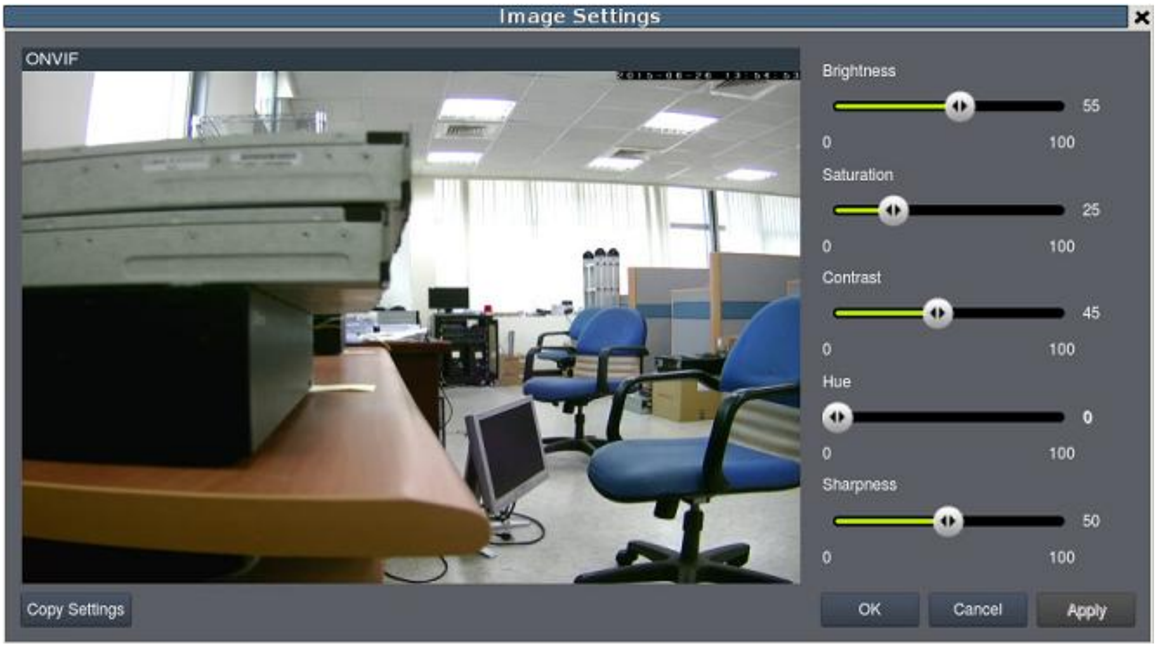


6.3.4. Others

Image Settings

Camera image settings can also be accessed by right-clicking the panel containing the camera video and selecting **Others > Image Settings**.





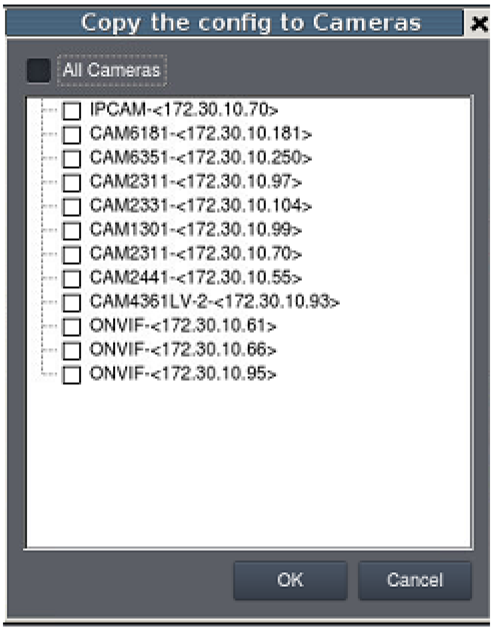
Brightness 55 (0–100)
Saturation 25 (0–100)
Contrast 45 (0–100)
Hue 0 (0–100)
Sharpness 50 (0–100)

1. Adjust the following sliders to change the camera image:
   - **Brightness** – The overall lighting level of the image. This value can be used to boost or reduce the apparent lighting of the image.
   - **Saturation** – The overall color intensity of the image. This value can be used to boost or reduce overall color intensity.

- **Contrast** – The lighting difference between dark and light areas of the image. This value can be used to boost or reduce apparent differences in lighting.
- **Hue** – The color cast of the image. This value can be used to compensate for colored lighting or other color casting.
- **Sharpness** – The edge contrast of the image. This value can be used to make the picture appear clearer.

2. Click **OK** to save your changes.

3. Click **Copy Settings** to have the same settings applied to other cameras. Once **Copy Settings** button is clicked, the following window will appear. Select the cameras you'd like to have the same settings applied to save time.



Copy the config to Cameras

□ All Cameras

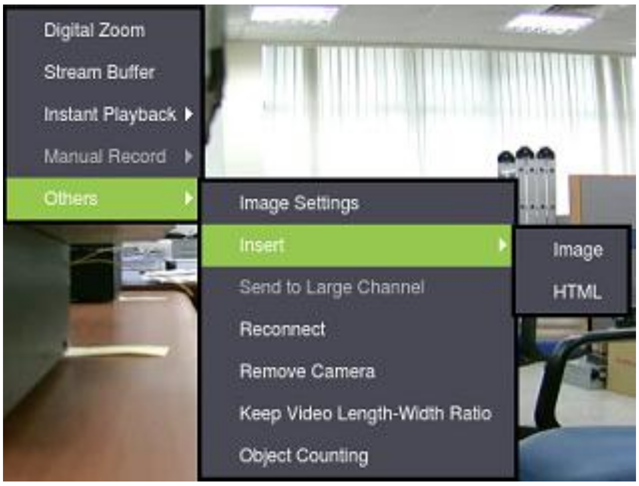
□ IPCAM-<172.30.10.70>
□ CAM6181-<172.30.10.181>
□ CAM6351-<172.30.10.250>
□ CAM2311-<172.30.10.97>
□ CAM2331-<172.30.10.104>
□ CAM1301-<172.30.10.99>
□ CAM2311-<172.30.10.70>
□ CAM2441-<172.30.10.55>
□ CAM4361LV-2-<172.30.10.93>
□ ONVIF-<172.30.10.61>
□ ONVIF-<172.30.10.66>
□ ONVIF-<172.30.10.95>

Note: Camera Image Settings can also be configured by right-click the camera entry in the *Camera List below the Live View*, then click **Image > Image**.

Insert

Image overlay

The panel can be replaced with a user overlay.



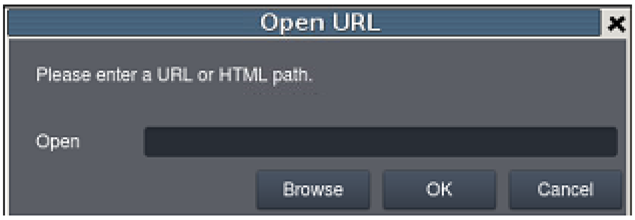
To overlay an image on top of a panel:

1. Right-click the panel and choose **Others** > **Insert** > **Image.** The system will prompt you to choose an image file.
2. Choose an image file, valid image types are JPEG, BMP, TIF, PNG. Click **Open** to open the file.
3. The image will be displayed in the panel. Click the red X in the top-right corner to close the image.

HTML Overlay

The HTML overlay function allows simple integration of web applications in the VMS by replacing one or more panels of the screen with an active browsing window. To overlay an HTML form or website on top of a panel:

1. Right-click the panel and choose **Others** > **Insert** > **HTML**.

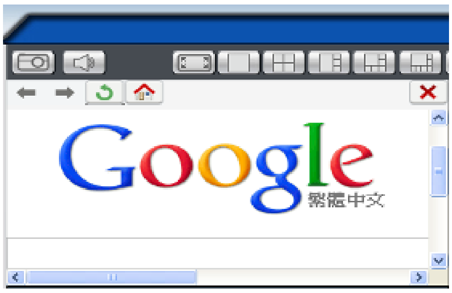

Open URL

Please enter a URL or HTML path.

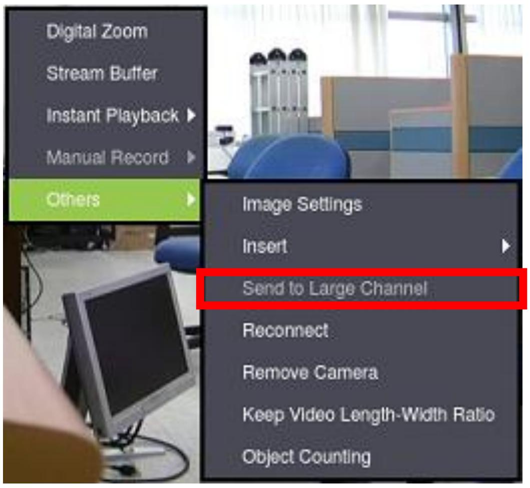
Open

2. In the field, enter a URL or the path containing the HTML form. You may also choose to click **Browse** and choose an HTML file.

3. The HTML or website will be displayed in the panel. Click the red X in the top-right corner to close the image.

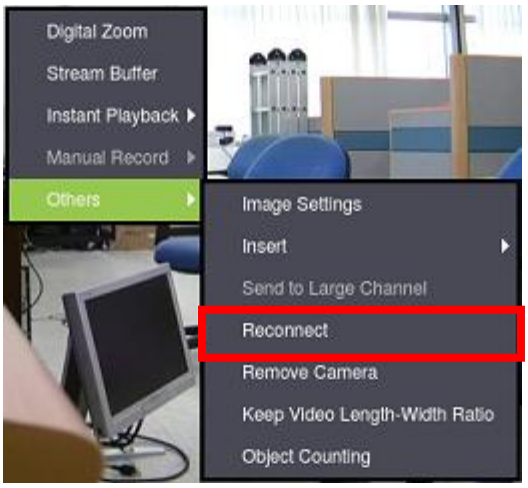


Send to Large Channel



When the view with different sizes is selected, views in smaller divisions can be switched to the larger division. To perform this action, right-click the panel corresponding to the camera and choose **Others > Send to Large Channel.**

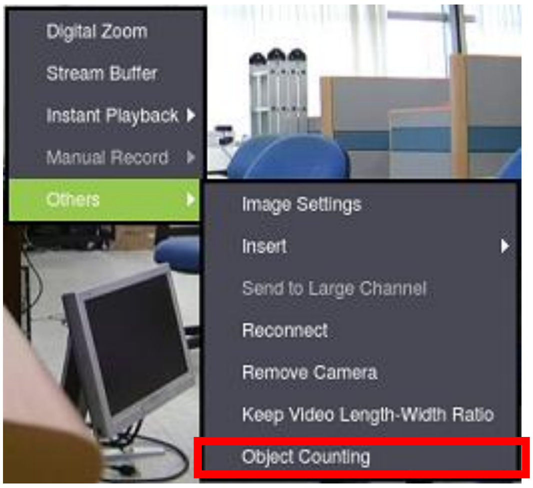
Reconnect



In some cases it may be necessary to manually reset the connection to a camera. To perform this action, right-click the panel corresponding to the camera and choose **Others > Reconnect.**

Remove the Camera

The Cameras can be removed by clicking **Others > Remove Camera**.

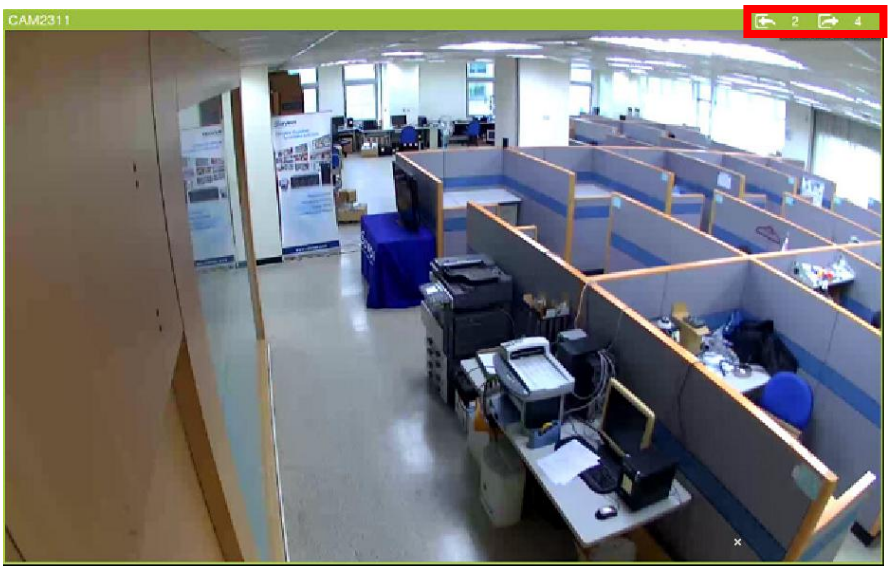


Keep Video Length-Width Ratio / Resize to Fit Window

The image can be set as the length-width ratio or resize to fit window by clicking **Others > Keep Video Length-Width Ratio / Resize to Fit Window.**

Object Counting (can only be set via remote client)

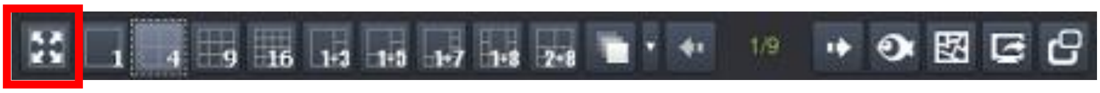
Object Counting result can be displayed (if it has been set) by clicking **Others > Object Counting**.



6.4. Full Screen View

6.4.1. Entering Full Screen View

From any view, you can switch to full screen mode by clicking on the full screen button located above the main viewing window. Optionally you may also choose to view a single frame in full screen mode by double clicking on the frame.



6.4.2. Exiting Full Screen Mode

To exit full screen mode, hit the **ESC** key on your keyboard.

Chapter 7. Server Setup

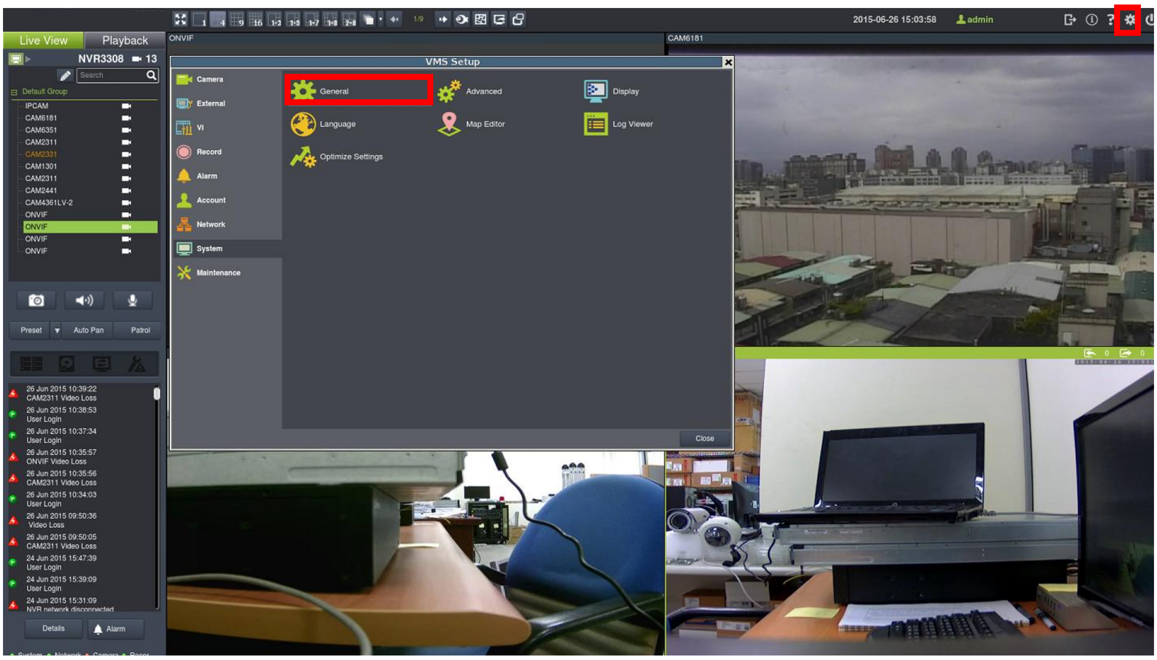
This section deals with Server setup procedures.

7.1. Server Settings

7.1.1. General Server Settings

The following sections deal with Server settings that can be configured under the *Server Settings* menu.

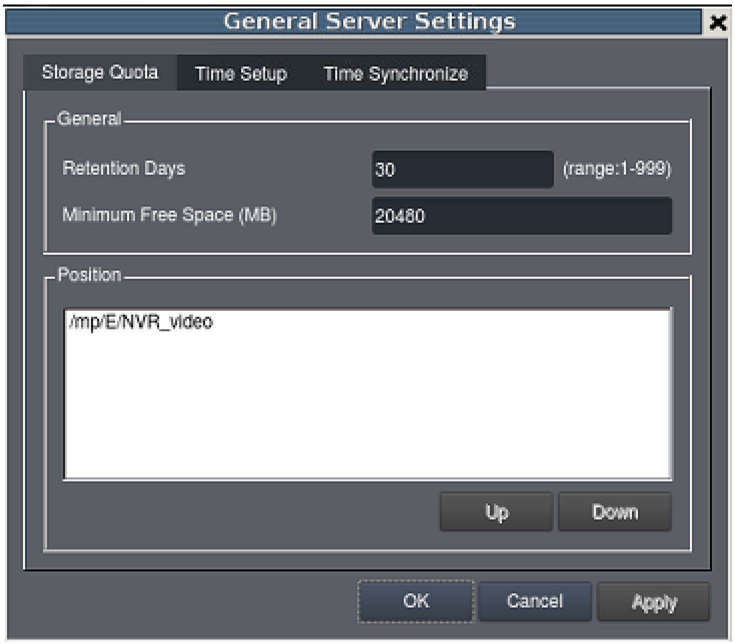
1. Click ⚙ to bring out **VMS Setup** window and select **System** and then select **General Server Settings**.



```
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
26 Jun 2015 09:50:36
 Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected
```

2. A tabbed window will appear providing the following configuration tabs: *Storage Quota and Time Settings.*

■ Storage Quota



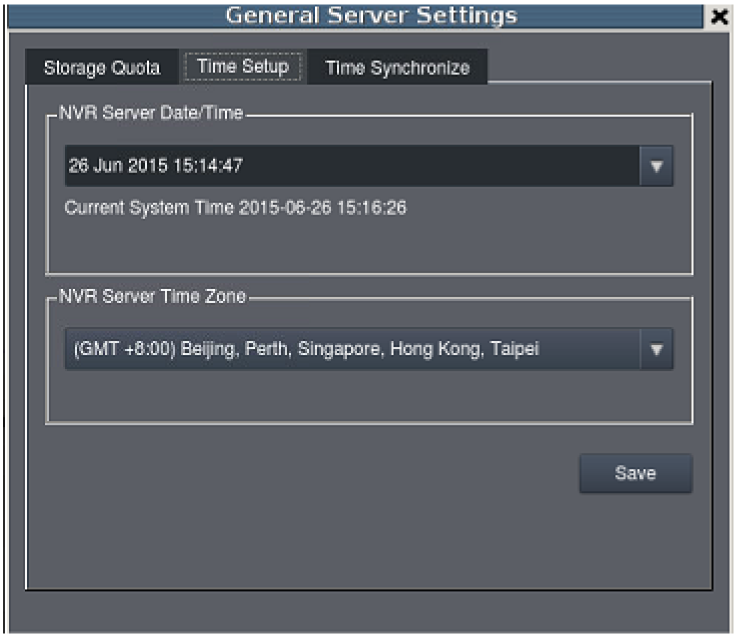
Retention Days: 30 (range:1-999)

Minimum Free Space (MB): 20480

/mp/E/NVR_video

In the **Minimum Free Space** field, the Minimum space required for storage is shown. The storage will be last for 30 days. Click on the items in the Position section and use the **Up** and **Down** buttons to change the storage priorities.

■ Time Setup



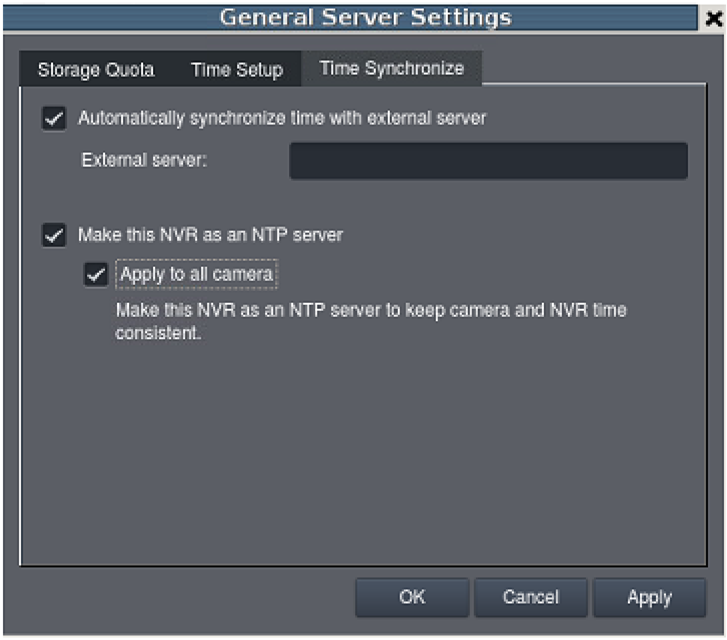
26 Jun 2015 15:14:47

Current System Time 2015-06-26 15:16:26

(GMT +8:00) Beijing, Perth, Singapore, Hong Kong, Taipei

To set the server time click on the number you wish to change and enter a value. Click **OK** to preserve the setting. The default time is set according to the real-time clock on server.

■ Time Synchronize



General Server Settings

☑ Automatically synchronize time with external server

External server:

☑ Make this NVR as an NTP server

☑ Apply to all camera

Make this NVR as an NTP server to keep camera and NVR time consistent.

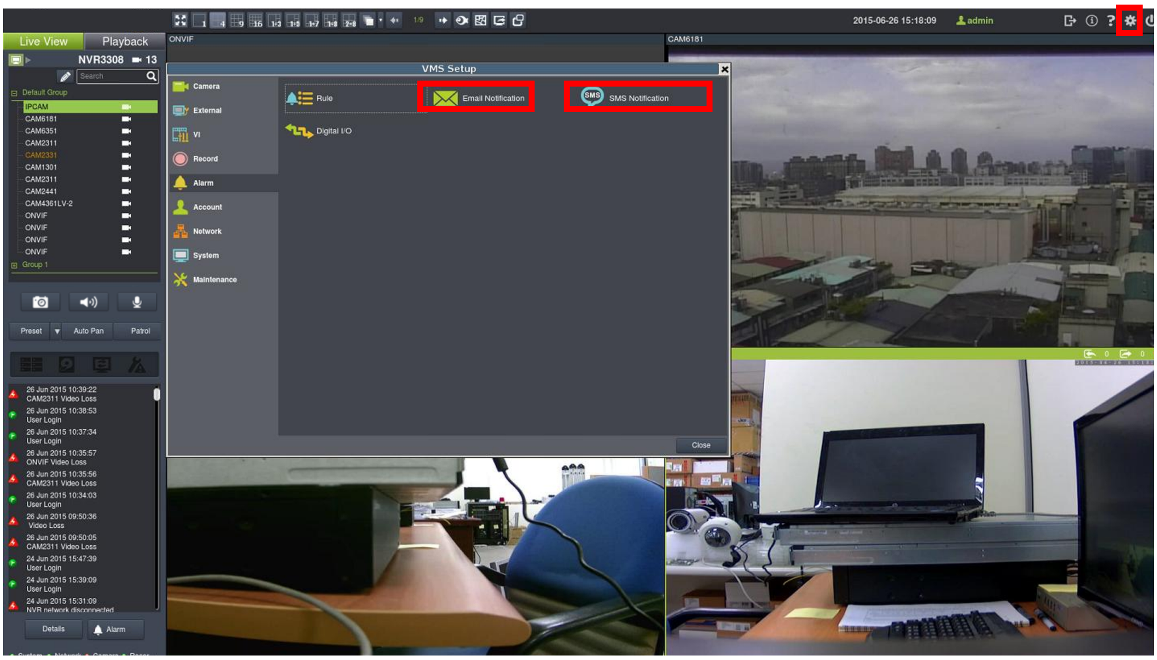
To synchronize the system time with the external server, check the option ”Automatically synchronize time with external server” to enable this functionality. And input the IP address of the external server in the External Server field.

Check the option “Make this NVR as an NTP server” to enable this functionality.

And check the option “Apply to all camera” to make this NVR as an NTP server and to have camera time and NVR time synchronized.

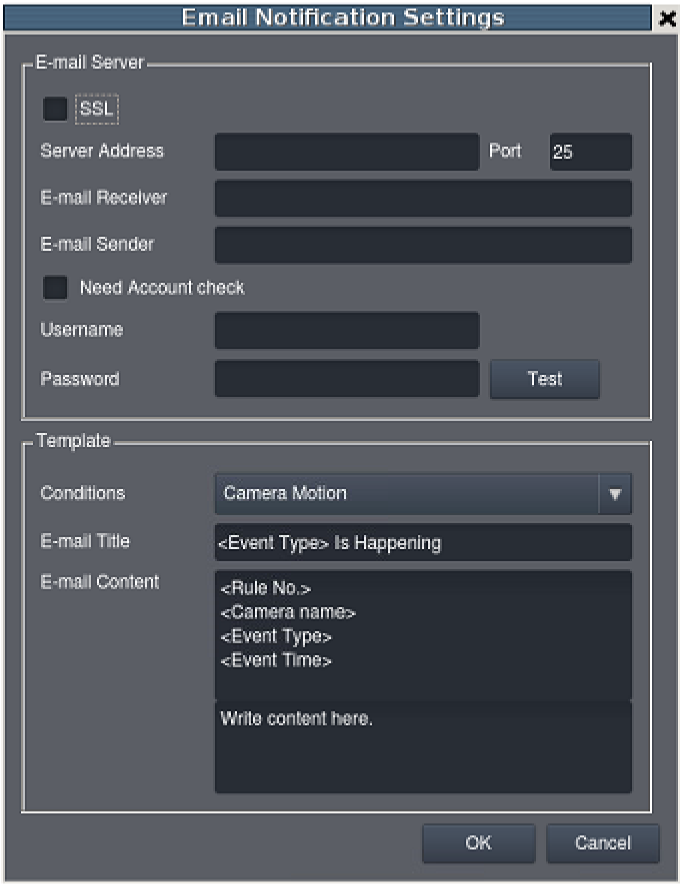
7.1.2. To perform Notification Setting

1. Click ⚙ to bring out **VMS Setup** window and select **Alarm** and then select **Email Notification** or **SMS Notification**.



26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
26 Jun 2015 09:50:36
Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected

2. Click **Email Notification** tab to continue.



Port: 25

Conditions: Camera Motion

E-mail Title: <Event Type> Is Happening

E-mail Content:
<Rule No.>
<Camera name>
<Event Type>
<Event Time>

Write content here.

SSL: Tick this option to enable SSL (Secure Sockets Layer) and to enhance security.

Server Address: You may either enter the URL (such as smtp.abc.com) or IP address of the SMTP server that the Server will use to deliver E-mail notifications. The SMTP server configured here must support Unicode Transformation Format-8 (UTF-8) encoding.

E-mail Receiver: Enter one or more E-mail addresses in the **Recipients:** field. These address(es) will receive notifications from the Server. Multiple addresses can be entered by separating individual addresses with semi - colons “;”.

E-mail Sender: Enter a valid E-mail address in the field. This address will be the default sender listed in E-mails sent from the Server.

Need Account Check: Tick this option to check.

Username: Enter the user name for the Server email account in the **Username** field.

Password: Enter the password for the Server email account in the **Password** field.

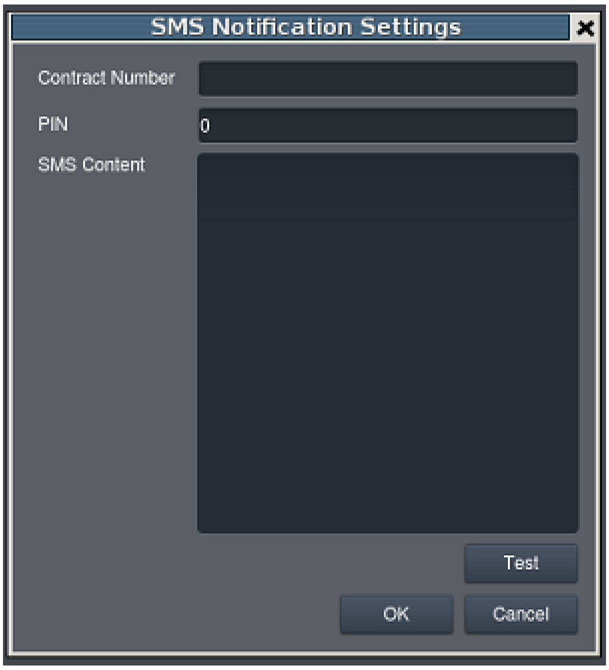
(Optional) Click **Test** to send a test message to the E-mail addresses listed.

Conditions: Select a condition from the dropdown list to send out an email notification.

E- Mail Title: Enter the subject of your notification E-mails, e.g., Server-xxxsite1notification in the field.

E- Mail Content: Enter a short message in the large field to describe the Server or a surveillance network.

3. Click the **SMS Notification** to continue.



Contact Number: Enter the phone numbers that will receive SMS notifications. Be sure to include the area code, e.g., “86”, in front of phone numbers. Use commas, “,” to separate individual phone numbers.

(Optional) If a SIM PIN is required, enter the PIN code in the **PIN** field. Note that applying incorrect PIN code may disable your SIM card.

Note: To change the PIN code, remove the SIM card from your GSM modem. Use a cell phone to change the PIN code and then re -install SIM card into the GSM modem. Changing PIN codes is not recommended because a configuration failure may disable your SIM card.

SMS Content: Type a simple description to include in the outgoing SMS messages

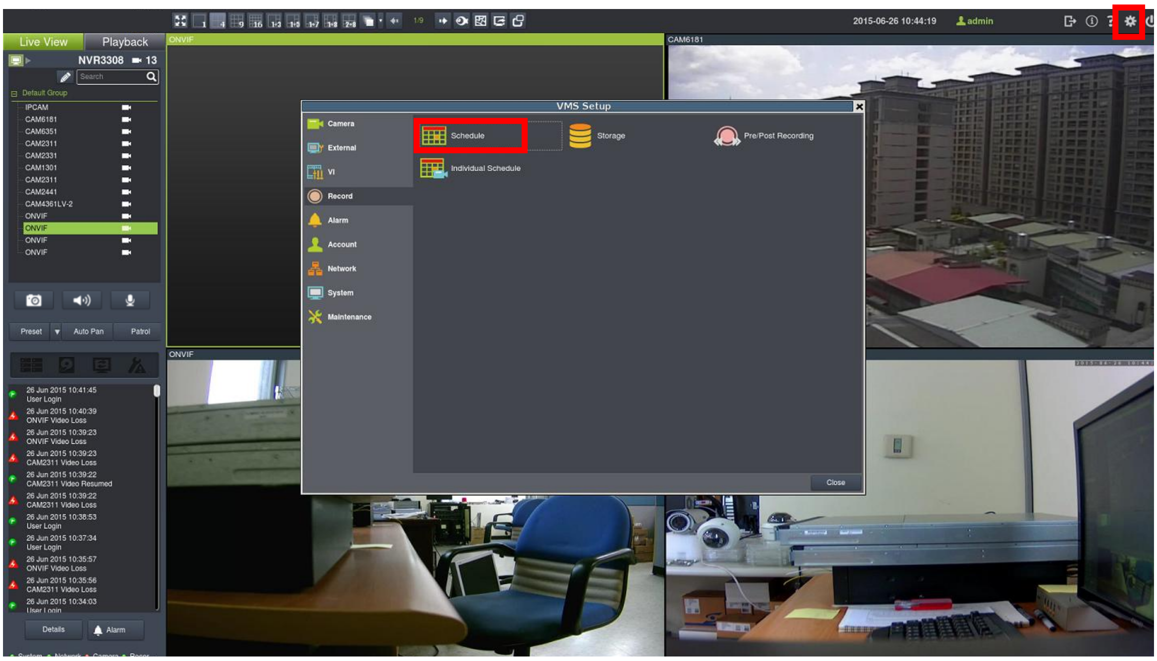
(Optional) Click **Test** to send a test message to the phone numbers listed.

Click the **Apply** button to apply the changes.

Click the **OK** button to exit E-mail/SMS settings.

7.1.3. Scheduling Recording

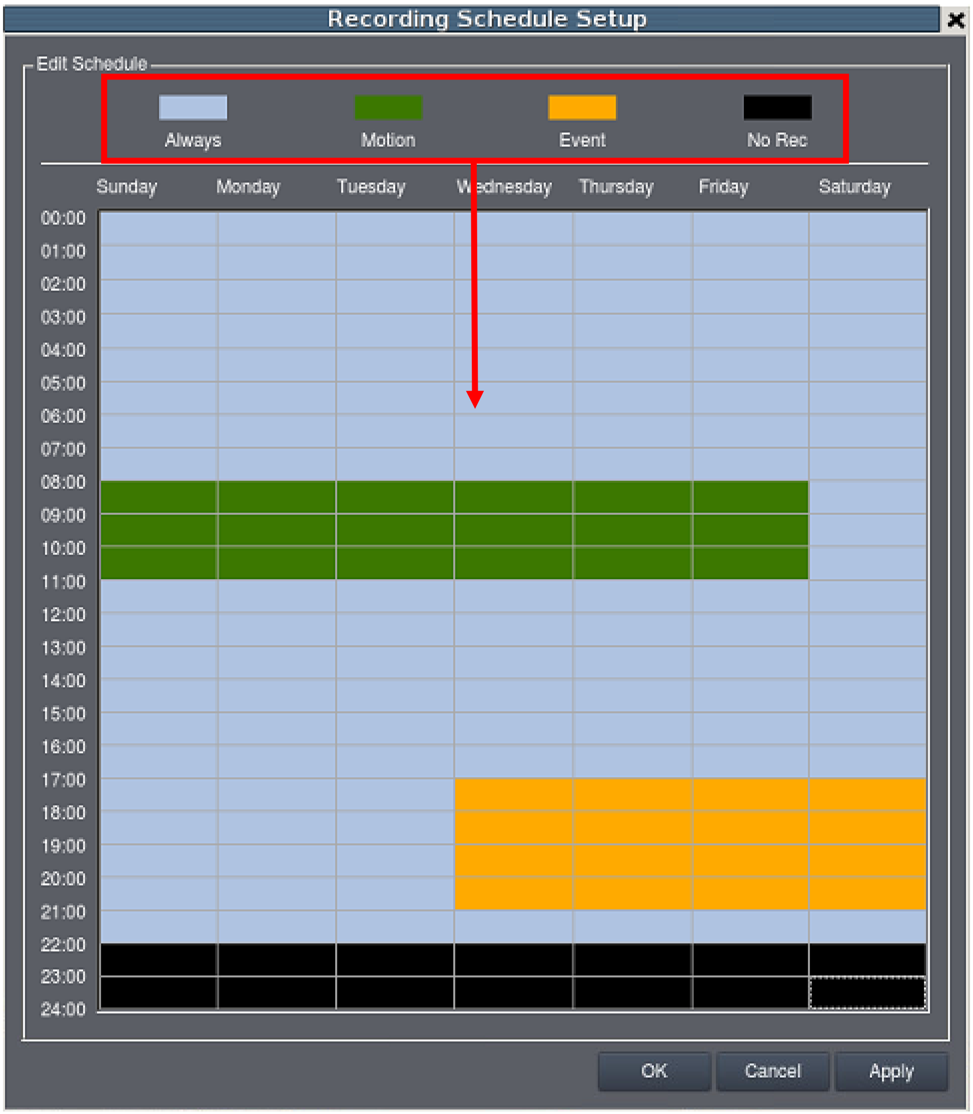
Click ⚙ to bring out **VMS Setup** window and select **Recording** and then **Schedule**.



```
26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
```

The schedule grid corresponds to every hour in the week. Click on one of the 2 recording methods and then click on the grid area to “paint in” the method for the corresponding hour.

1. Click **OK** to save the settings and exit the dialog.

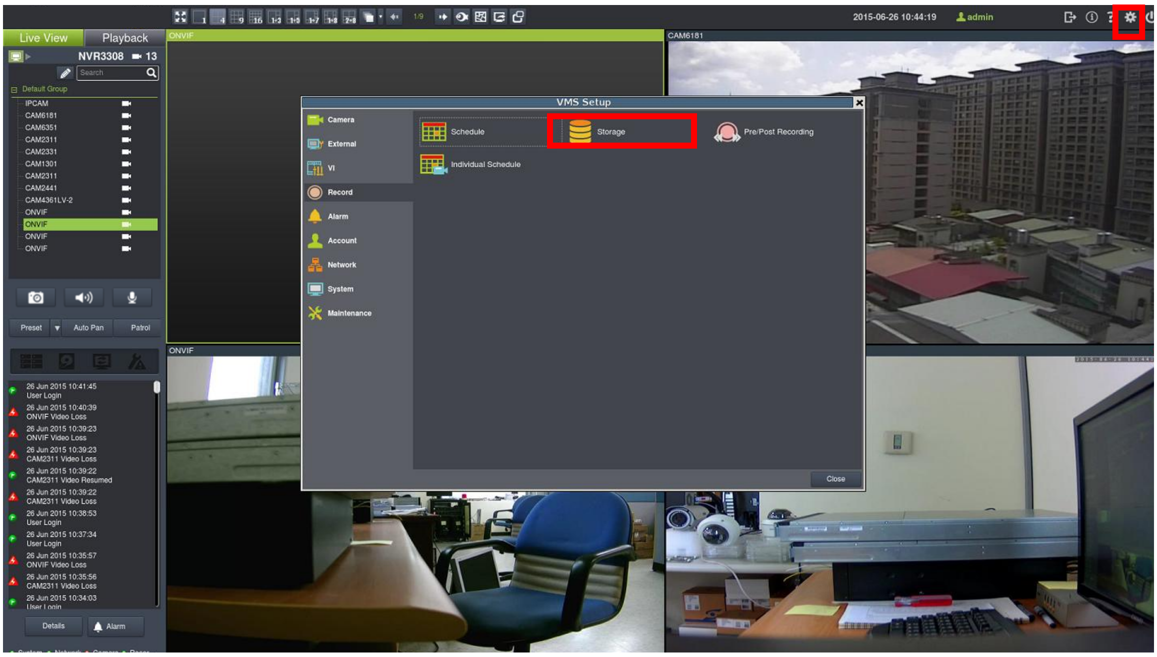


🟦 Always 🟩 Motion 🟧 Event ⬛ No Rec

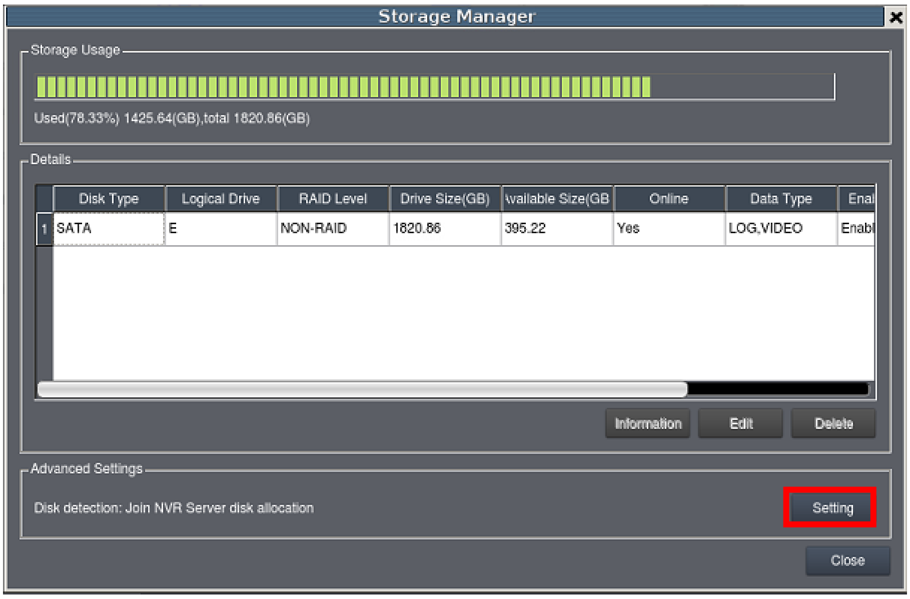
	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
01:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
02:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
03:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
04:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
05:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
06:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
07:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
08:00	🟩	🟩	🟩	🟩	🟩	🟩	🟦
09:00	🟩	🟩	🟩	🟩	🟩	🟩	🟦
10:00	🟩	🟩	🟩	🟩	🟩	🟩	🟦
11:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
12:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
13:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
14:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
15:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
16:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
17:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
18:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
19:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
20:00	🟦	🟦	🟦	🟧	🟧	🟧	🟧
21:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
22:00	⬛	⬛	⬛	⬛	⬛	⬛	⬛
23:00	⬛	⬛	⬛	⬛	⬛	⬛	⬛
24:00							

7.1.4. Storage Management

1. To access the information about the drives configured in your Server, click to bring out **VMS Setup** window and then select **Recording** to see and click **Storage** option for **Storage Manager**.



2. All available Logical Drives, as well as their sizes, free space, and status will appear. Click target drive and then **Setting** to set the log and location for saving the video recordings.



Storage Manager

Storage Usage

Used(78.33%) 1425.64(GB),total 1820.86(GB)

Details

	Disk Type	Logical Drive	RAID Level	Drive Size(GB)	\vailable Size(GB	Online	Data Type	Enal
1	SATA	E	NON-RAID	1820.86	395.22	Yes	LOG,VIDEO	Enabl

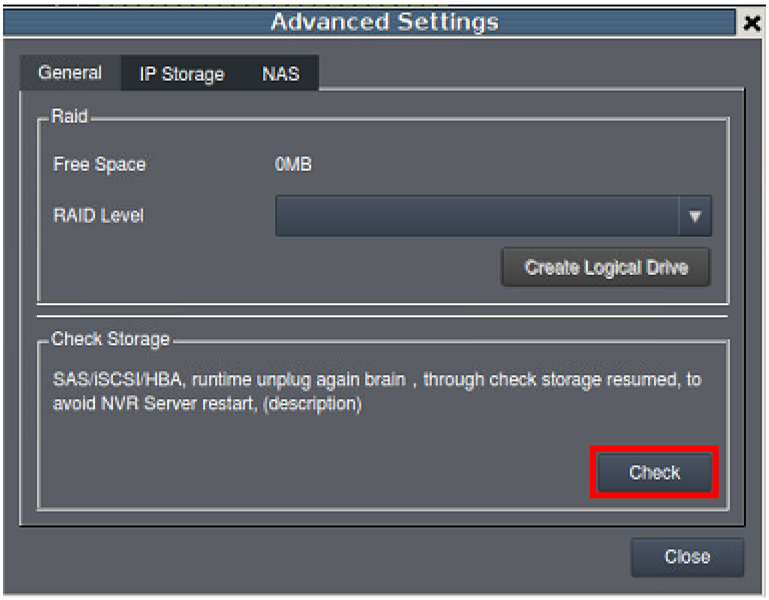
Information   Edit   Delete

Advanced Settings

Disk detection: Join NVR Server disk allocation   Setting

Close

3. Click the target drive first and then **Settings**. In “General” tab, click **Check**.

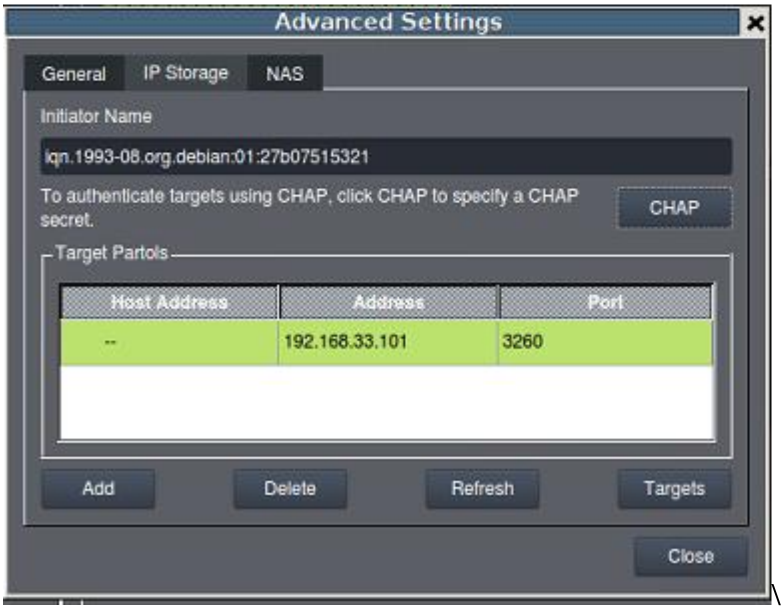


Free Space 0MB

SAS/iSCSI/HBA, runtime unplug again brain , through check storage resumed, to avoid NVR Server restart, (description)

4. Choose the RAID level, and then click **Create Logical Drive** to create the RAID configuration. The system supports recording to ISCSI and NAS.

5. In “IP Storage” tab, you can authenticate targets by clicking CHAP to setup CHAP.

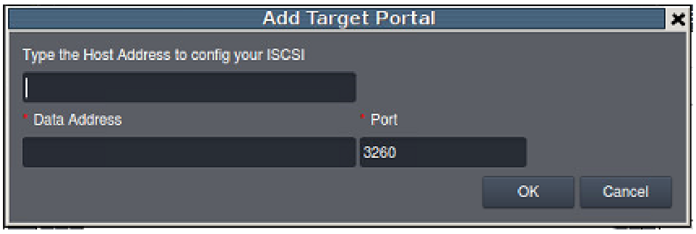


Initiator Name: iqn.1993-08.org.debian:01:27b07515321

To authenticate targets using CHAP, click CHAP to specify a CHAP secret.

Host Address	Address	Port
--	192.168.33.101	3260

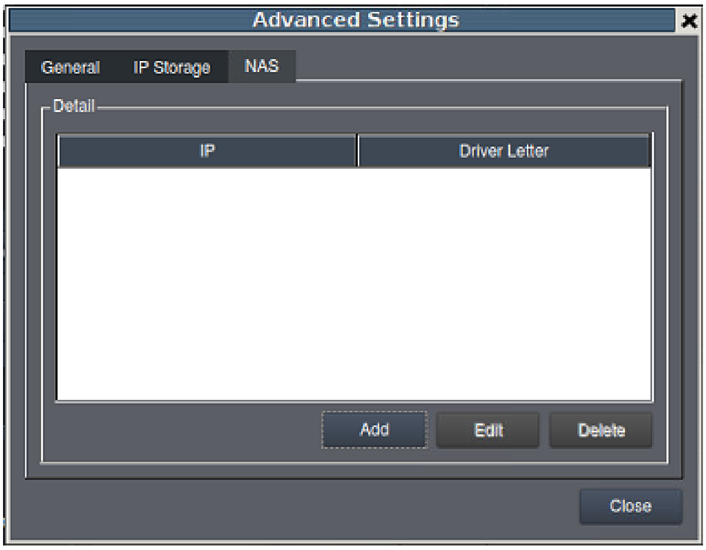
- Add: Clicking Add and input the required information to add more targets.



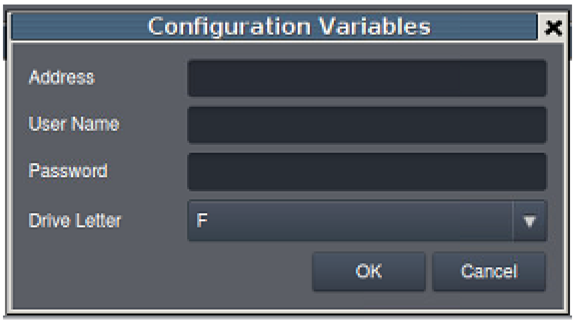
Port: 3260

- Delete: Clicking Delete to delete the selected.
- Refresh: Clicking Refresh to refresh.
- Target: Click Targets to see the setup result.

6. In “NAS” tab, you can add NAS in as the video storage.



Clicking Add and input the required information to add NAS as the video storage.

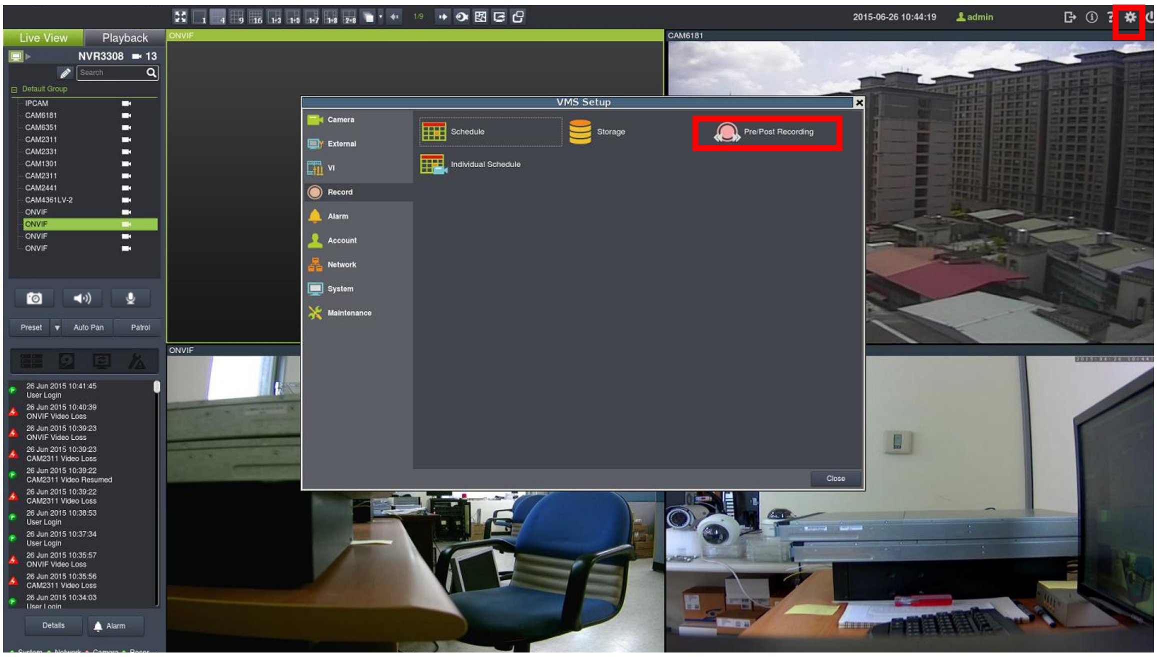


Drive Letter: F

7.1.5. Pre/Post Recording

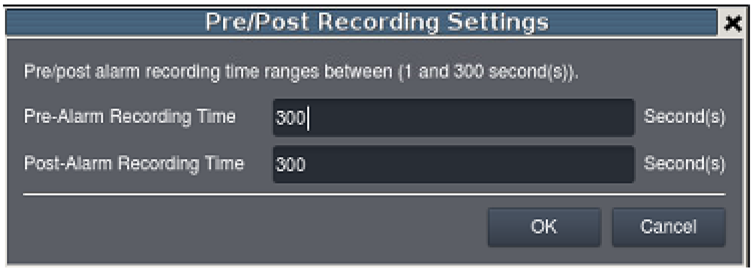
Video streams are constantly processed and cached in memory. The Server can trace back and preserve video/images from several minutes before and after the occurrence of an alarm.

Click to bring out **VMS Setup** window and select **Recording** and then select **Pre/Post Recording** .



```
26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
```

The following pop-up window will appear:



Pre/Post Recording Settings

Pre/post alarm recording time ranges between (1 and 300 second(s)).

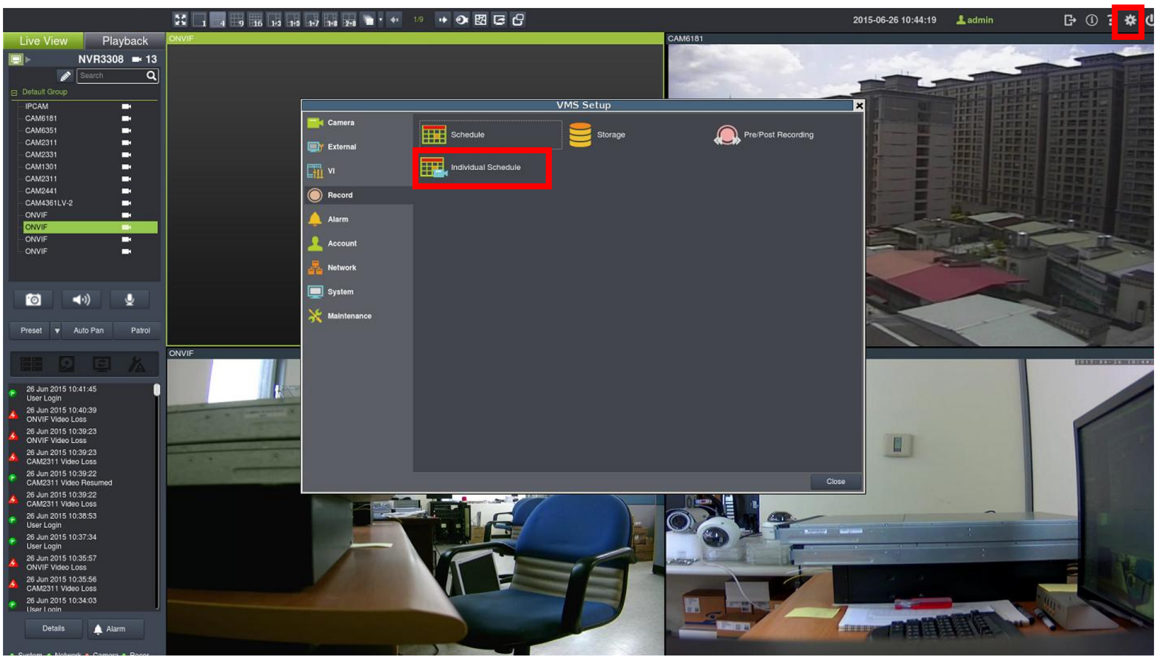
Pre-Alarm Recording Time 300 Second(s)

Post-Alarm Recording Time 300 Second(s)

In each of the boxes enter values for the Pre and Post Recording times from 1 to 300 seconds (default is 300 seconds). Click the **OK** button to finish the process.

7.1.6. Individual Schedule

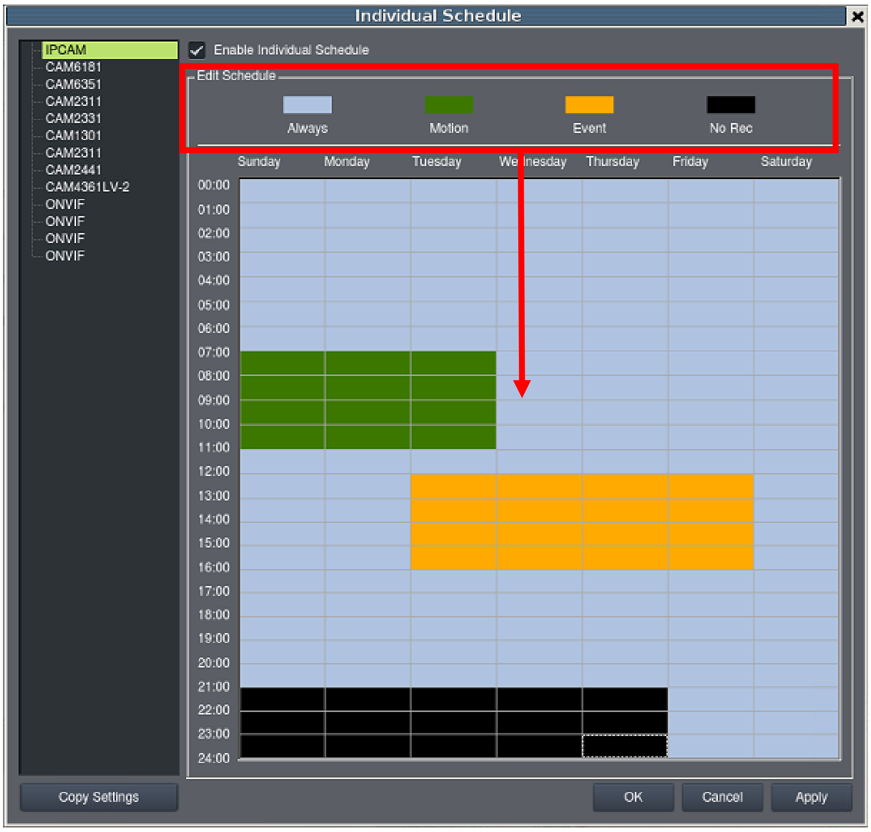
Schedules can be set for individual camera. Click ⚙ to bring out **VMS Setup** window and select **Recording** and then select **Individual Schedule**.



```
26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
```

The following pop-up window will appear:

The schedule grid corresponds to every hour in the week. Click on one of the 2 recording methods and then click on the grid area to “paint in” the method for the corresponding hour. Click **OK** to save the settings and exit the dialog.



Individual Schedule

- IPCAM
- CAM6181
- CAM6351
- CAM2311
- CAM2331
- CAM1301
- CAM2311
- CAM2441
- CAM4361LV-2
- ONVIF
- ONVIF
- ONVIF
- ONVIF

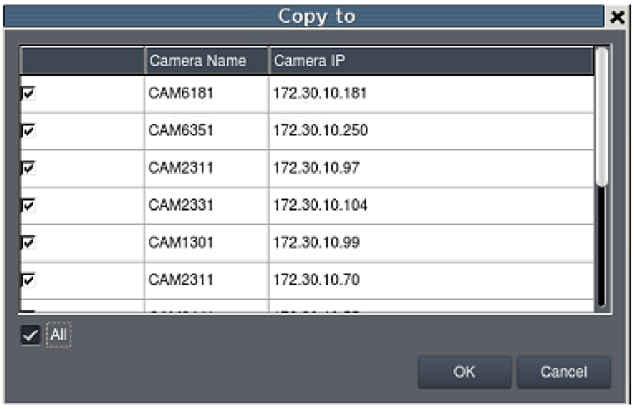
☑ Enable Individual Schedule

Edit Schedule

🟦 Always 🟩 Motion 🟧 Event ⬛ No Rec

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
01:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
02:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
03:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
04:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
05:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
06:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
07:00	🟩	🟩	🟩	🟦	🟦	🟦	🟦
08:00	🟩	🟩	🟩	🟦	🟦	🟦	🟦
09:00	🟩	🟩	🟩	🟦	🟦	🟦	🟦
10:00	🟩	🟩	🟩	🟦	🟦	🟦	🟦
11:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
12:00	🟦	🟦	🟧	🟧	🟧	🟧	🟦
13:00	🟦	🟦	🟧	🟧	🟧	🟧	🟦
14:00	🟦	🟦	🟧	🟧	🟧	🟧	🟦
15:00	🟦	🟦	🟧	🟧	🟧	🟧	🟦
16:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
17:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
18:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
19:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
20:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
21:00	⬛	⬛	⬛	⬛	⬛	🟦	🟦
22:00	⬛	⬛	⬛	⬛	⬛	🟦	🟦
23:00	⬛	⬛	⬛	⬛	⬛	🟦	🟦
24:00							

Click **Copy Settings** to have the same settings applied to other cameras.
Once **Copy Settings** button is clicked, the following window will appear. Select the cameras you’d like to have the same settings applied to save time.



Copy to

	Camera Name	Camera IP
☑	CAM6181	172.30.10.181
☑	CAM6351	172.30.10.250
☑	CAM2311	172.30.10.97
☑	CAM2331	172.30.10.104
☑	CAM1301	172.30.10.99
☑	CAM2311	172.30.10.70

☑ All

Chapter 8. Camera Setup

This section deals with Camera setup procedures. These options can be accessed by right-clicking the Camera entry in the *Camera List below the Live View*.

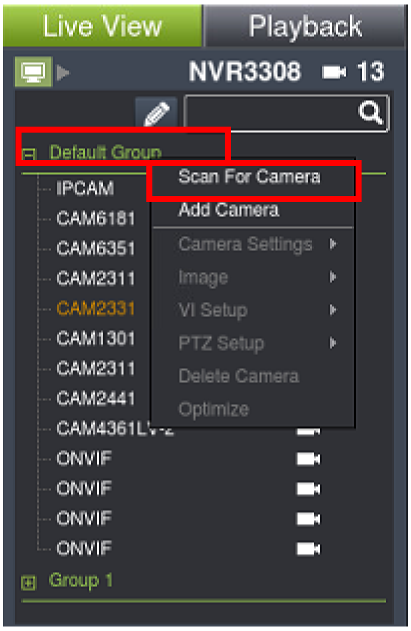
8.1. Adding Cameras

Cameras can be added to the Server in two ways: via an automatic scan or by manually inputting the camera information.

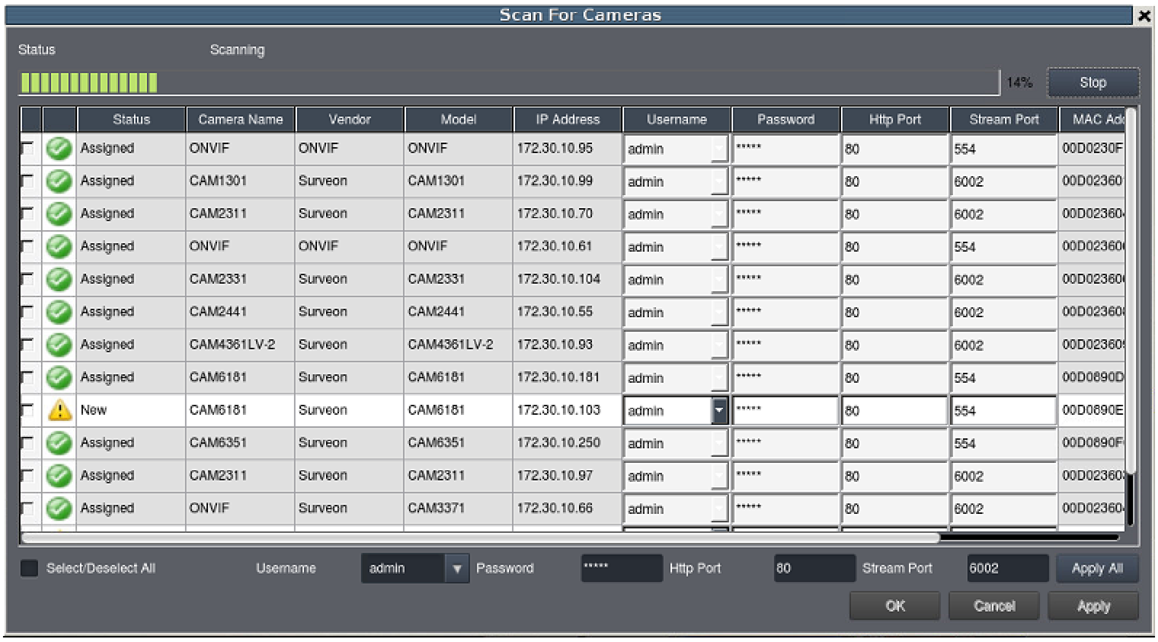
8.1.1. Automatic Scan for Cameras

To begin an automatic scan for cameras:

Right-click on the **Default Group** to bring out the setting menu and select **Scan for Cameras**.



1. The system will respond by beginning an automatic scan. Once the scan is complete, the cameras that can be added to the Server will be displayed. Information available for each camera will include:



Scan For Cameras

Status Scanning

14% Stop

		Status	Camera Name	Vendor	Model	IP Address	Username	Password	Http Port	Stream Port	MAC Ad
□	✓	Assigned	ONVIF	ONVIF	ONVIF	172.30.10.95	admin	*****	80	554	00D0230F
□	✓	Assigned	CAM1301	Surveon	CAM1301	172.30.10.99	admin	*****	80	6002	00D02360
□	✓	Assigned	CAM2311	Surveon	CAM2311	172.30.10.70	admin	*****	80	6002	00D02360
□	✓	Assigned	ONVIF	ONVIF	ONVIF	172.30.10.61	admin	*****	80	554	00D02360
□	✓	Assigned	CAM2331	Surveon	CAM2331	172.30.10.104	admin	*****	80	6002	00D02360
□	✓	Assigned	CAM2441	Surveon	CAM2441	172.30.10.55	admin	*****	80	6002	00D02360
□	✓	Assigned	CAM4361LV-2	Surveon	CAM4361LV-2	172.30.10.93	admin	*****	80	6002	00D02360
□	✓	Assigned	CAM6181	Surveon	CAM6181	172.30.10.181	admin	*****	80	554	00D0890D
□	⚠	New	CAM6181	Surveon	CAM6181	172.30.10.103	admin	*****	80	554	00D0890E
□	✓	Assigned	CAM6351	Surveon	CAM6351	172.30.10.250	admin	*****	80	554	00D0890F
□	✓	Assigned	CAM2311	Surveon	CAM2311	172.30.10.97	admin	*****	80	6002	00D02360
□	✓	Assigned	ONVIF	Surveon	CAM3371	172.30.10.66	admin	*****	80	6002	00D02360

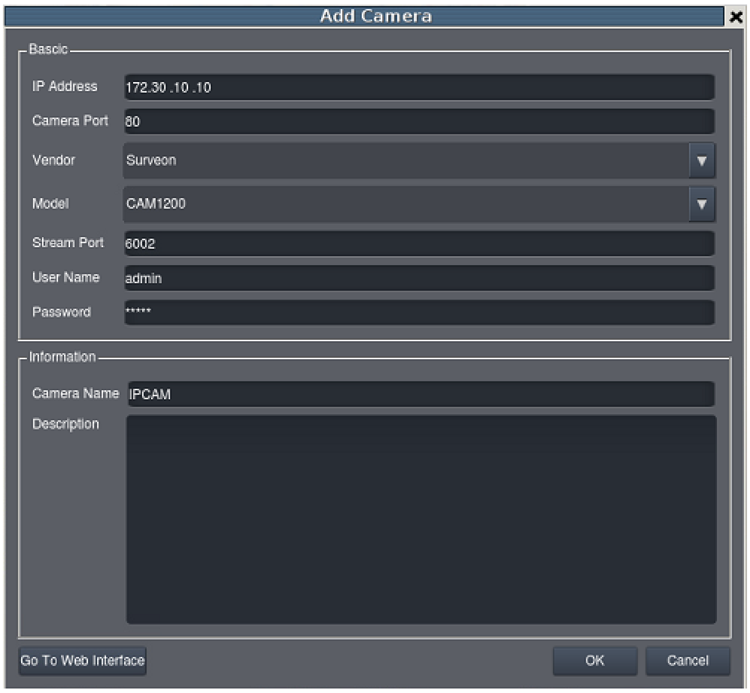
□ Select/Deselect All   Username admin   Password *****   Http Port 80   Stream Port 6002

- **Status** – The camera will display *New* if it has not been added to this Server, otherwise it will display *Assigned*.
- **Camera Name** – The default camera name (Make/Model)
- **Vendor - Including ACTI, Afreey, AXIS, Arecont, BOSCH, Dahua, Dynacolor, EDIMAX, EverFocus, HIKVISION, IQinvision, JVC, LG, Panasonic, Surveon, and ONVIF.**
- **Model**
- **IP Address**
- **Username**
- **Password**
- **Http Port**
- **Stream Port**
- **MAC Address**

2. To add a camera to the system, check the box by the camera entry. You may also check the **Select All** box at the bottom of the window to select all the cameras found.

Enter the username and password, and press **Apply Selected**. Click **OK** to add the selected cameras to the Server.

3. (Optional) Double-click any camera entry to bring up the camera detail page. From this page you may change the following information:



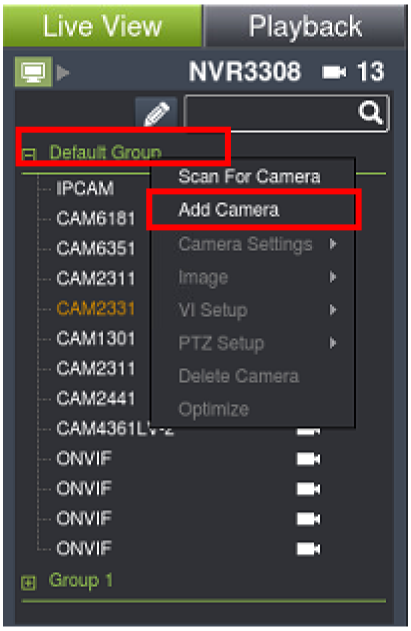
IP Address 172.30 .10 .10
Camera Port 80
Vendor Surveon
Model CAM1200
Stream Port 6002
User Name admin
Password *****
Camera Name IPCAM
Description

- **IP Address** – Changing this value will affect connectivity.
- **Camera Port -** The web access port, default is 80.
- **Vendor** – Changing this value will affect connectivity.
- **Model** – Changing this value will affect connectivity.
- **Stream Port** – Default is 6002.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Information**
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

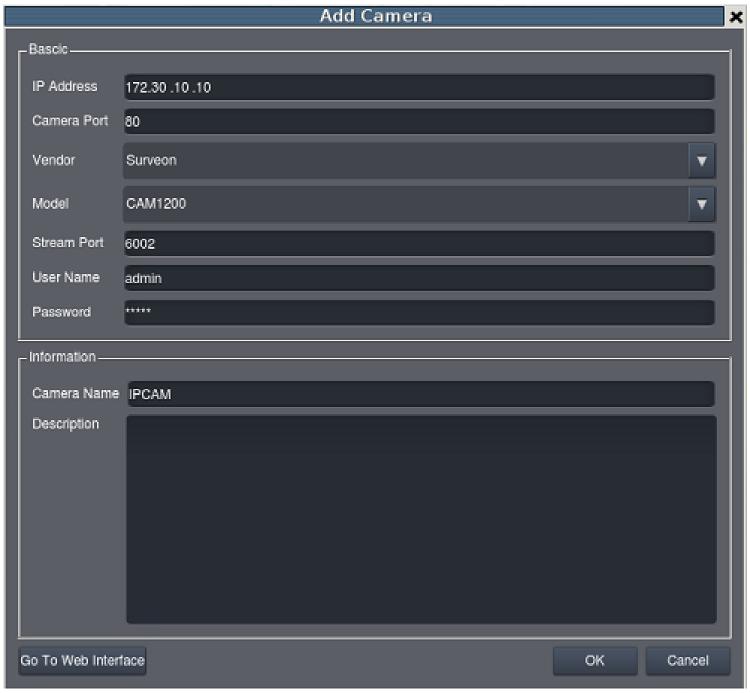
8.1.2. Manually Adding Cameras

To manually add a camera to the Server:

Right-click on the camera to bring out the setting menu and select **Add Camera**.



2. In the camera window fill out the following information:



Add Camera

Basic

IP Address: 172.30 .10 .10

Camera Port: 80

Vendor: Surveon

Model: CAM1200

Stream Port: 6002

User Name: admin

Password: *****

Information

Camera Name: IPCAM

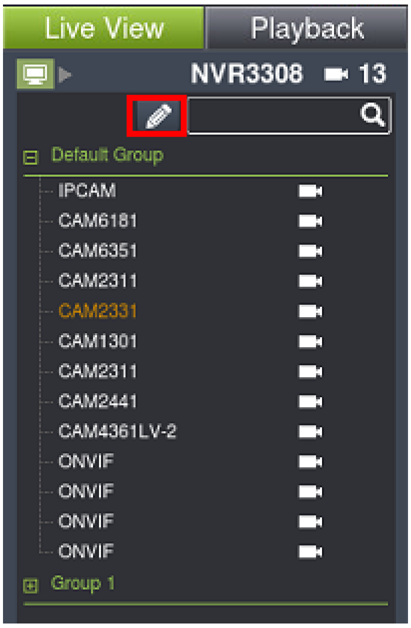
Description:

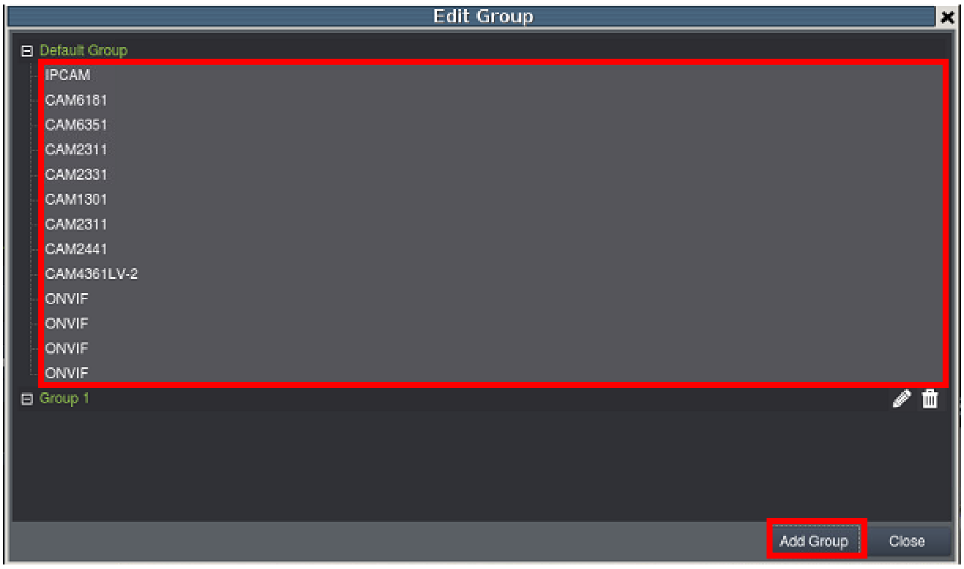
- **IP Address** – Changing this value will affect connectivity.

- **Camera Port -** The web access port, default is 80.
- **Vendor** – Changing this value will affect connectivity.
- **Model** – Changing this value will affect connectivity.
- **Stream Port** – Default is 6002.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Information**
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

8.1.3. Managing Group

To edit, add, and delete a group, click ✎ to bring out the editing window.



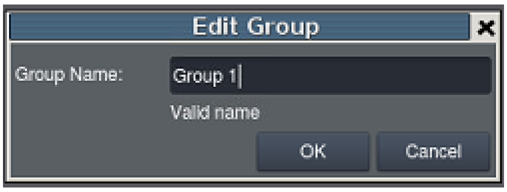


Add a group

1. Use the Shift button on the keyboard to select multiple cameras from the Default Group.

2. Click Add Group to add the selected ones as a group.

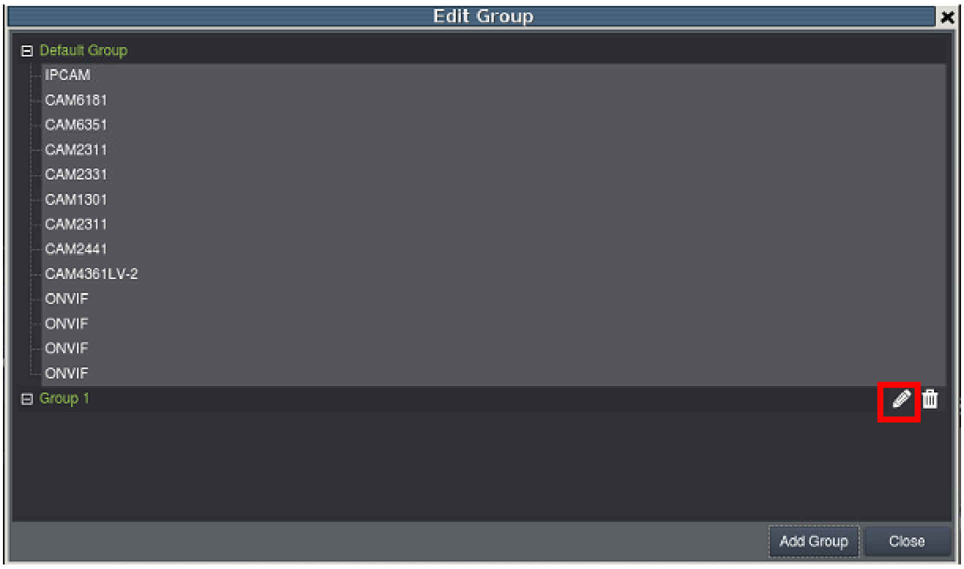
3. The system will ask for a group name. Input a group name and click OK.



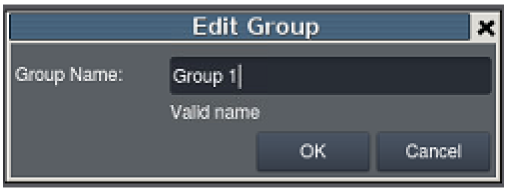
Group Name: Group 1

Valid name

Rename the group



1. To rename a group, click ✎ on the group you'd like to rename to bring out the editing window.

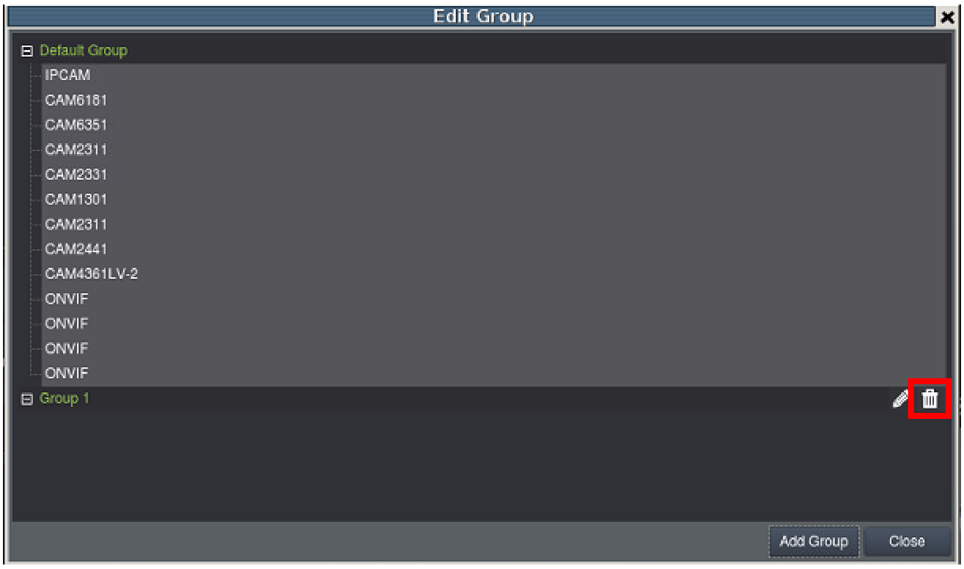


Group Name: Group 1

Valid name

2. Input a new group name and click OK.

Delete the group



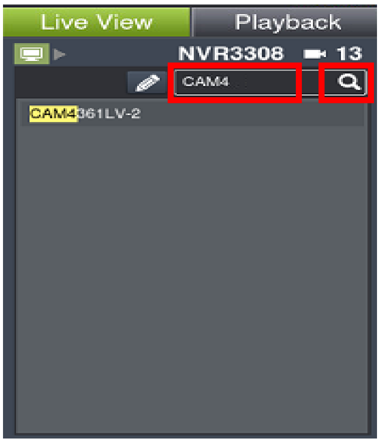
Default Group
- IPCAM
- CAM6181
- CAM6351
- CAM2311
- CAM2331
- CAM1301
- CAM2311
- CAM2441
- CAM4361LV-2
- ONVIF
- ONVIF
- ONVIF
- ONVIF

Group 1

1. To rename a group, click 🗑 on the group you'd like to delete.

8.1.4. Search camera

Input the query in the search box and click 🔍 to search from the added cameras.



CAM4

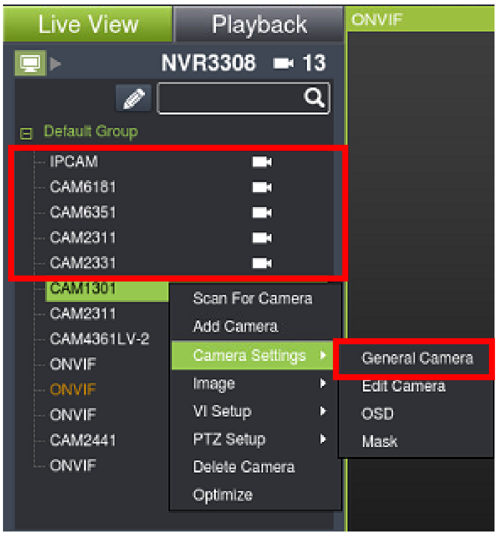
CAM4361LV-2

8.2. Camera General Settings

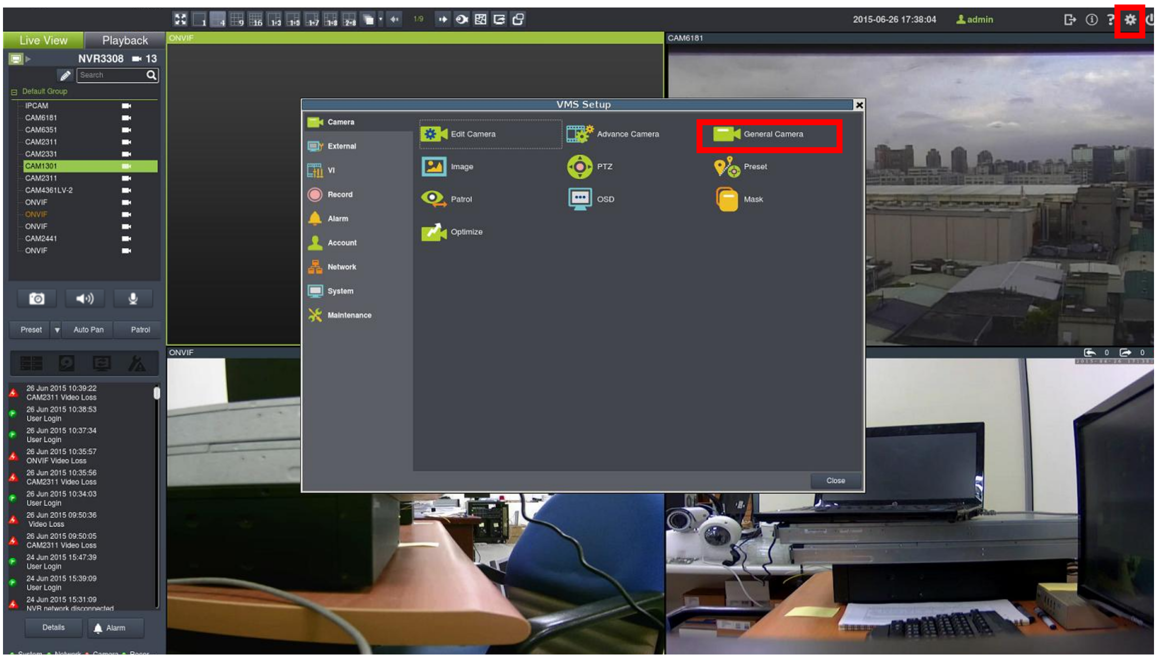
8.2.1. General Camera Settings

Camera general settings include network connectivity settings, as well as basic camera name, description and icon settings.

1. Right-click the camera entry and select **Camera Settings > General Camera**.

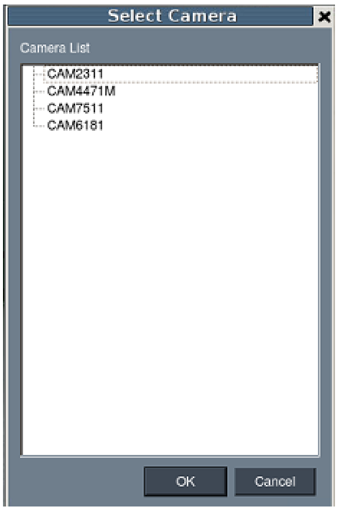


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **General Camera**.



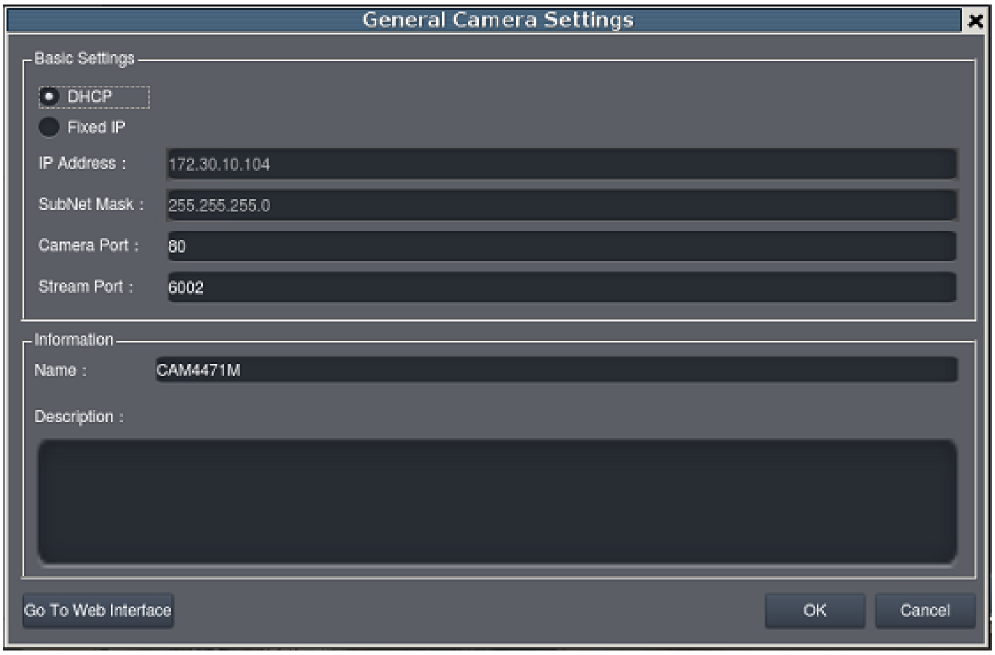
```
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
26 Jun 2015 09:50:36
 Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected
```

Select a specific camera for general setting.



- CAM2311
- CAM4471M
- CAM7511
- CAM6181

There are two ways to specify the IP address for the camera.



● DHCP
○ Fixed IP

IP Address : 172.30.10.104

SubNet Mask : 255.255.255.0

Camera Port : 80

Stream Port : 6002

Name : CAM4471M

Description :

- **If you wish to automatically assign an IP address to the camera, use DHCP services.**
- **If you wish to assign a fixed IP, select Fixed IP Address, and provide an IP address for the camera in the IP Address field. The Subnet Mask will be shown together with the IP address.**

1. You may continue by editing any of the following options:

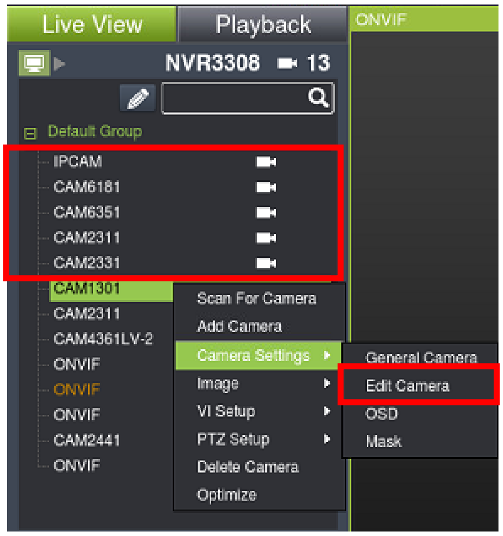
- **Subnet Mask -** a logically visible subdivision of an IP network.

- **Camera Port -** This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Stream Port -** This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**

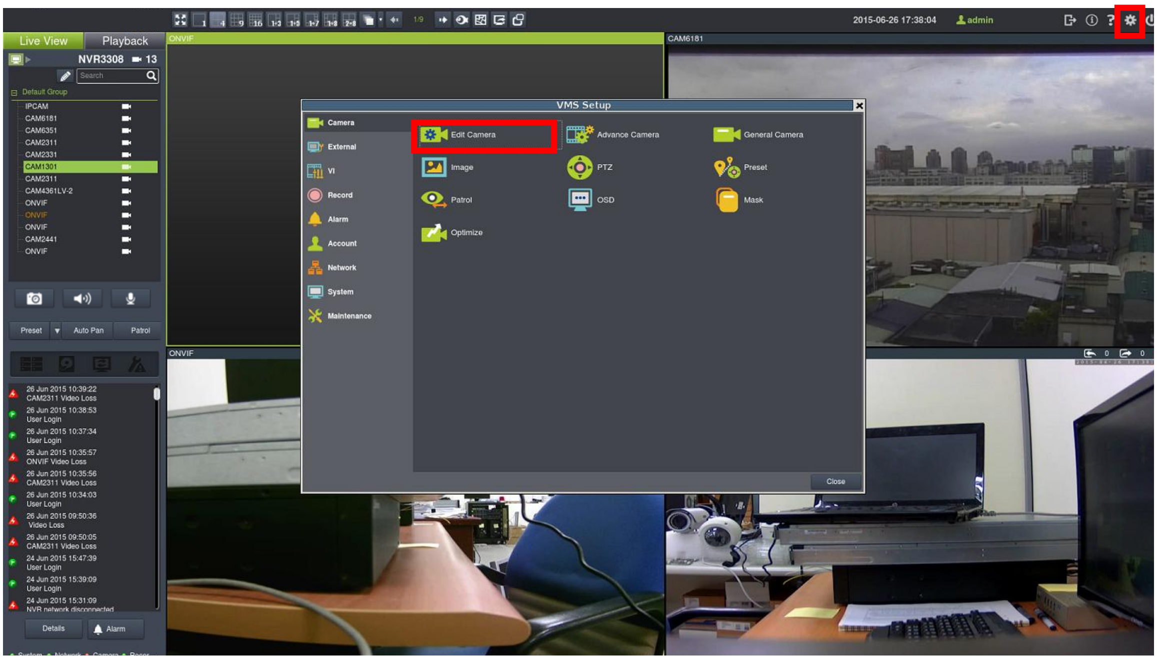
2. Click **OK** to save your changes.

8.2.2. Edit Camera

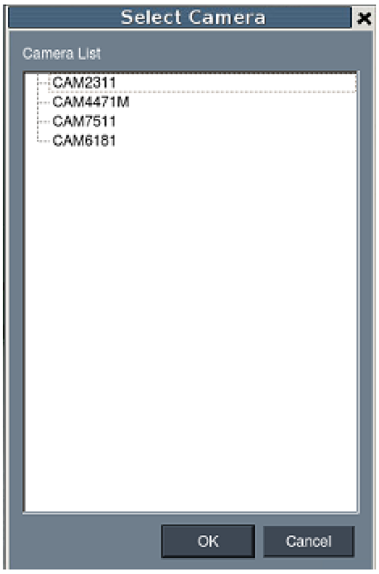
1. Right-click the camera entry and select **Camera Settings > Edit Camera** for settings to the selected camera.



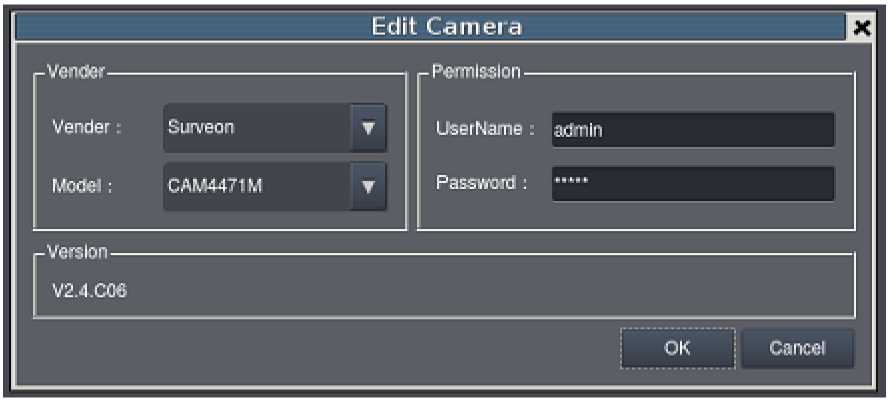
Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Edit Camera**.



Select a specific camera for editing.



2. In the *Permissions* section, enter a valid username in the **User Name** field and password in the **Password** field.



Vender : Surveon

Model : CAM4471M

UserName : admin

Password : *****

V2.4.C06

Note: The system will not perform an active check on the username and password. Setting an incorrect username or password may affect camera connectivity and configurability.

3. Changing the Camera Model and Vendor

In certain situations it may be necessary to change the Vendor or Model information for the camera. To perform this operation:

3.1. Select the new **Vendor** and **Model** from the respective drop-downs.

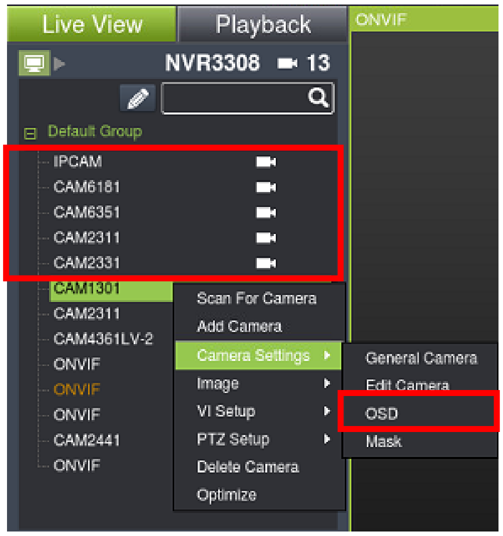
3.2. Click **OK** to save your changes.

Note: Setting an incorrect vendor or model may affect camera connectivity.

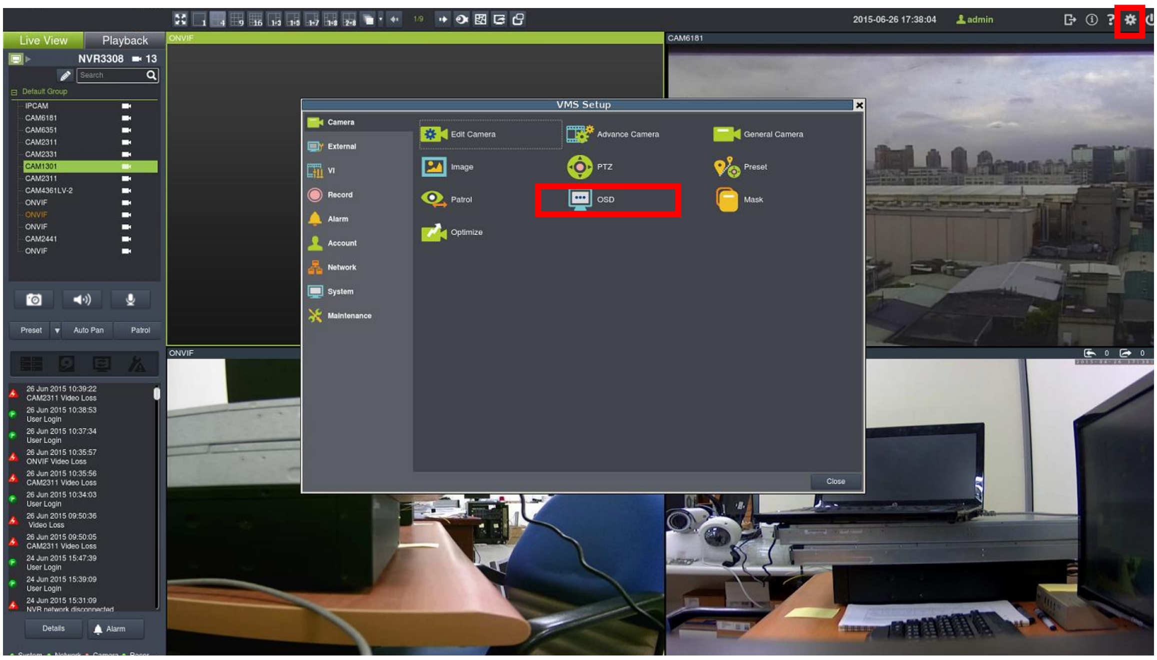
8.2.3. OSD Settings

On cameras with OSD capabilities, these capabilities can be configured within the server. To configure the information for the on-screen display:

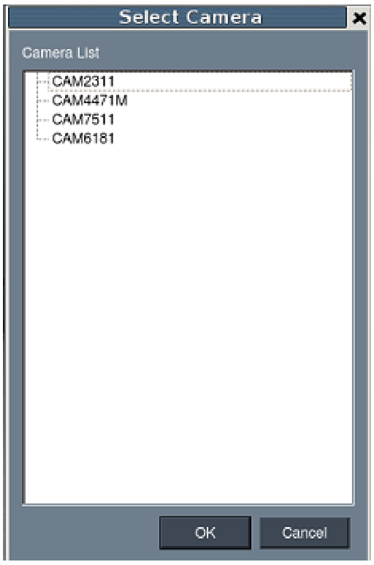
1. Right-click on the specific camera and select **Camera Settings > OSD** to bring out the OSD settings menu.



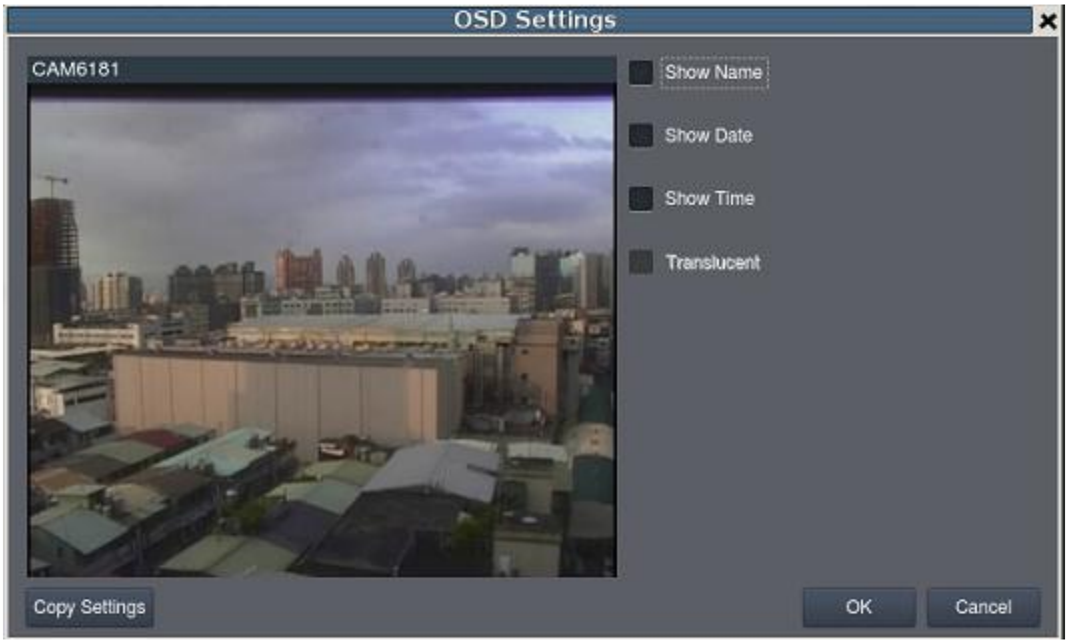
Or click to bring out **VMS Setup** window and select **Camera** and then select **OSD**.



Select a specific camera for OSD settings.

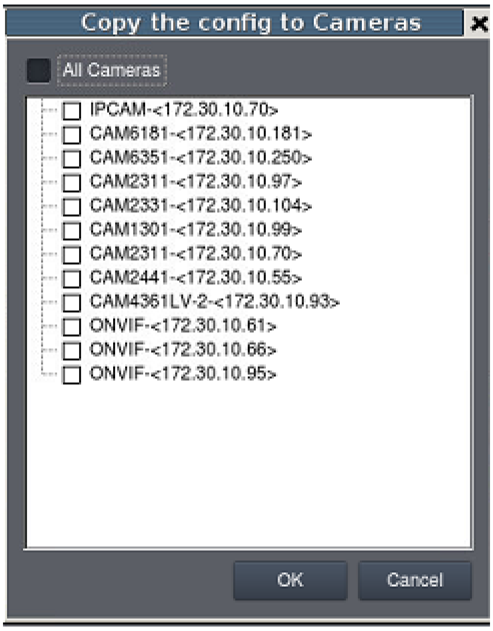


2. Choose any of the following options:



- **Show Name -** Displays the input text on video.
- **Show Date** – Displays the camera date.
- **Show Time** – Displays the camera time.
- Click **Copy Settings** to have the same settings applied to other cameras.

3. Once **Copy Settings** button is clicked, the following window will appear. Select the cameras you’d like to have the same settings applied to save time.



Copy the config to Cameras

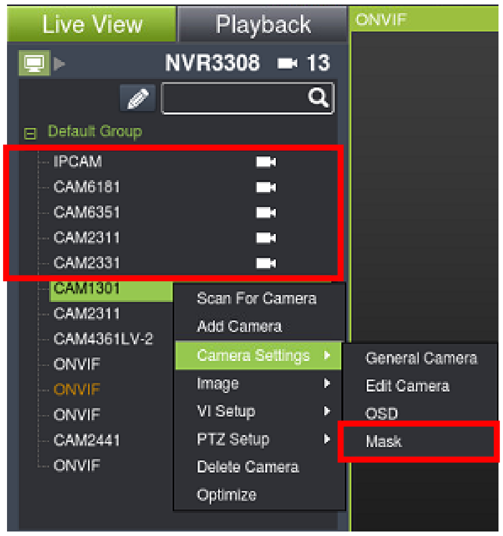
□ All Cameras

□ IPCAM-<172.30.10.70>
□ CAM6181-<172.30.10.181>
□ CAM6351-<172.30.10.250>
□ CAM2311-<172.30.10.97>
□ CAM2331-<172.30.10.104>
□ CAM1301-<172.30.10.99>
□ CAM2311-<172.30.10.70>
□ CAM2441-<172.30.10.55>
□ CAM4361LV-2-<172.30.10.93>
□ ONVIF-<172.30.10.61>
□ ONVIF-<172.30.10.66>
□ ONVIF-<172.30.10.95>

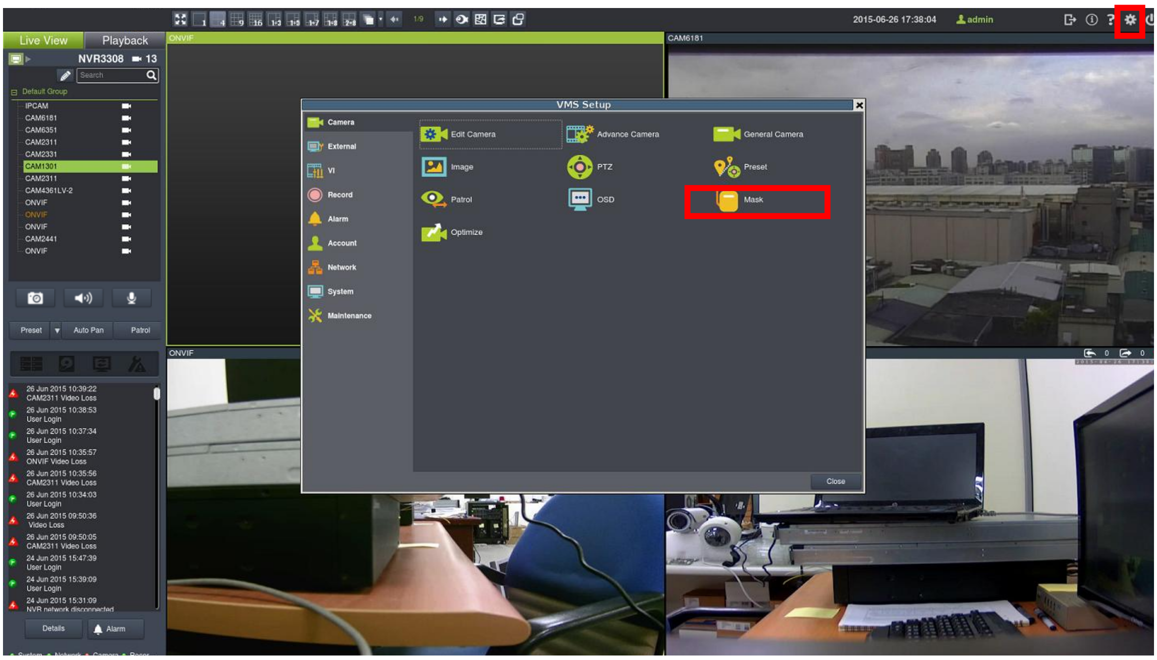
8.2.4. Privacy Mask Settings

Privacy masks can be added on the video:

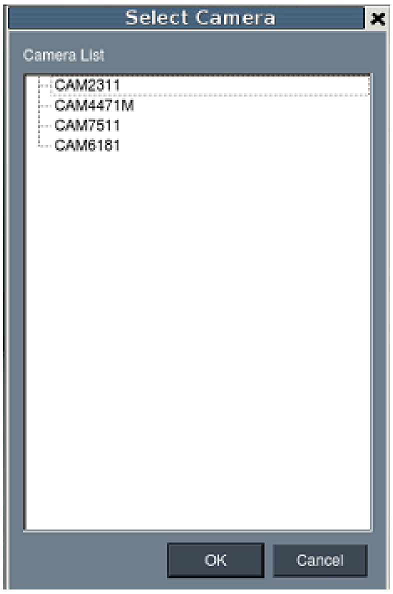
1. Right-click on the specific camera and select **Camera Settings > Mask** to bring out the privacy mask settings menu.

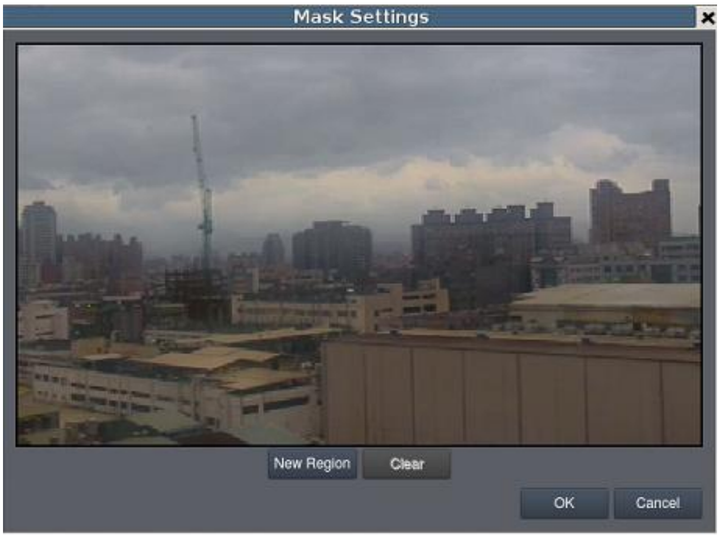


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Mask**.



Select a specific camera for Privacy Mask settings.





1. Click the New Region button to create a new privacy mask overlay, denoted by a border.

2. Click and drag the overlay to move the overlay around the screen. Click and drag one of the six dots on the border to resize and reshape the overlay. If multiple windows are present, the window being edited will have a red border.

3. Repeat these steps to create up to three windows. Click OK to save the privacy mask.

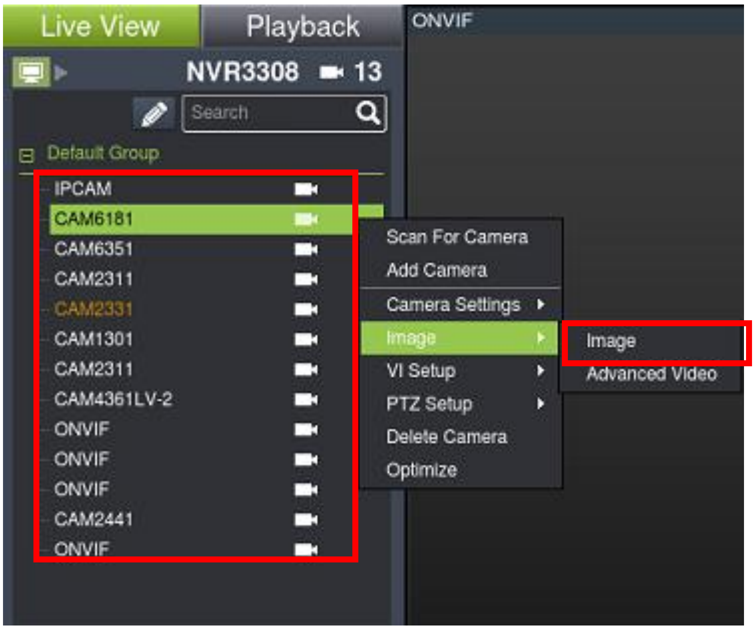
The masked areas will be shown in black on the live view screen after the mask is saved.

8.3. Camera Image and Quality Settings

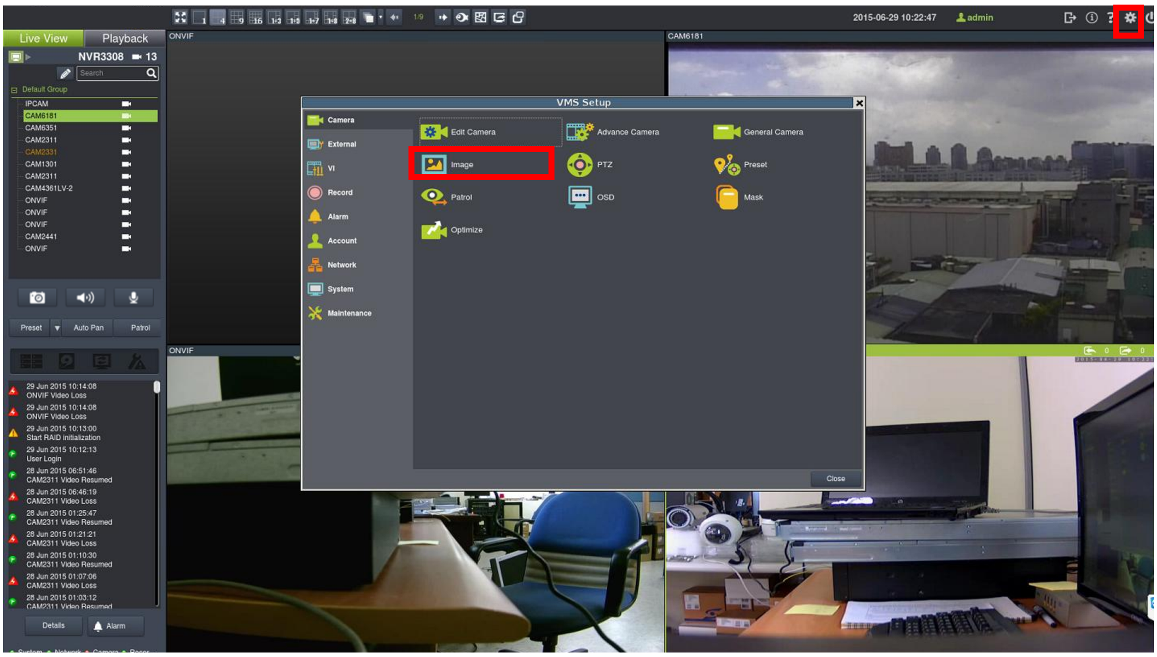
8.3.1. Camera Image Settings

To configure camera image settings:

Right-click the specific camera entry and click **Image > Image**.

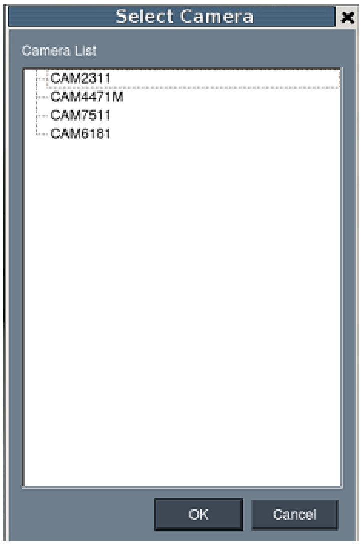


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Image.**



29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
28 Jun 2015 01:07:06
CAM2311 Video Loss
28 Jun 2015 01:03:12
CAM2311 Video Resumed

Select a specific camera for image settings.



Select Camera

Camera List

CAM2311
CAM4471M
CAM7511
CAM6181

Note: You must be logged into the camera before changing settings or else the operation will fail.

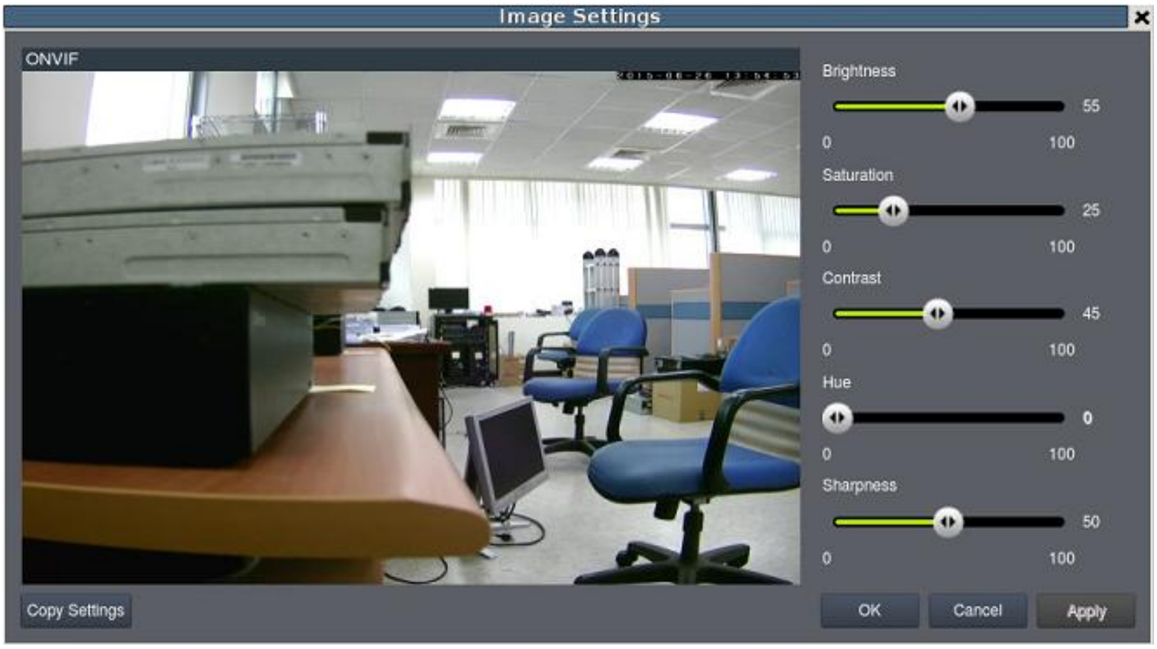


Image Settings

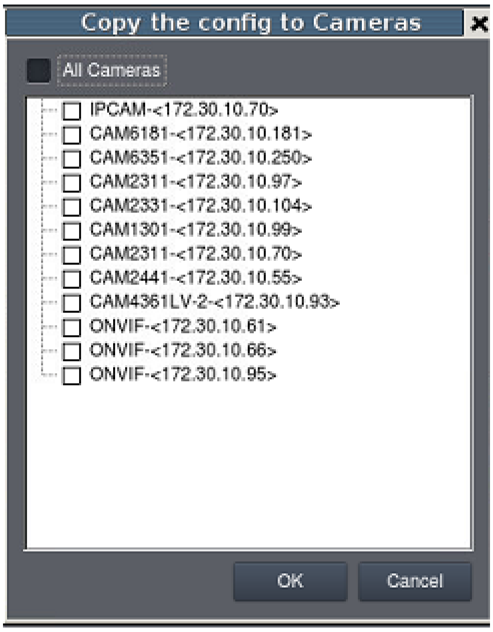
ONVIF

Brightness 55 (0–100)
Saturation 25 (0–100)
Contrast 45 (0–100)
Hue 0 (0–100)
Sharpness 50 (0–100)

1. Adjust the following sliders to change the camera image:
   - **Brightness** – The overall lighting level of the image. This value can be used to boost or reduce the apparent lighting of the image.
   - **Saturation** – The overall color intensity of the image. This value can be used to boost or reduce overall color intensity.

- **Contrast** – The lighting difference between dark and light areas of the image. This value can be used to boost or reduce apparent differences in lighting.
- **Hue** – The color cast of the image. This value can be used to compensate for colored lighting or other color casting.
- **Sharpness** – The edge contrast of the image. This value can be used to make the picture appear clearer.

2. Click **OK** to save your changes.
3. Click **Copy Settings** to have the same settings applied to other cameras.
   Once **Copy Settings** button is clicked, the following window will appear. Select the cameras you'd like to have the same settings applied to save time.

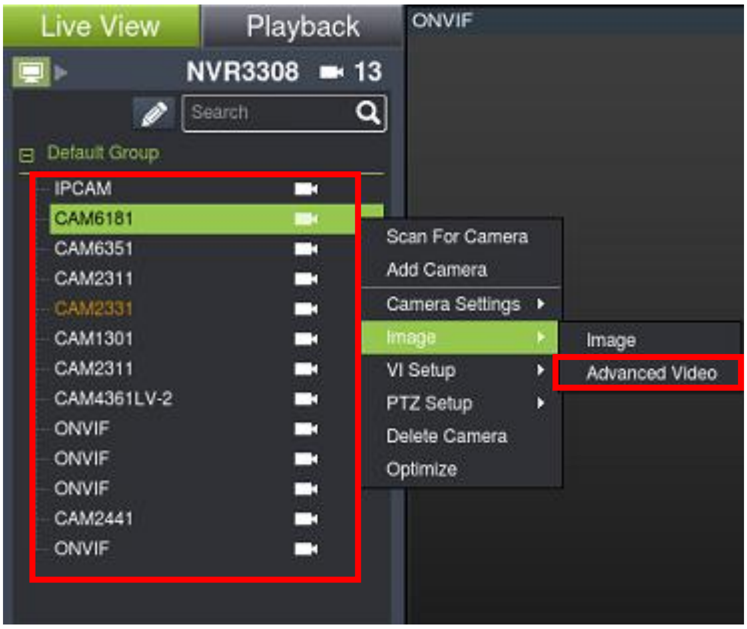


□ All Cameras

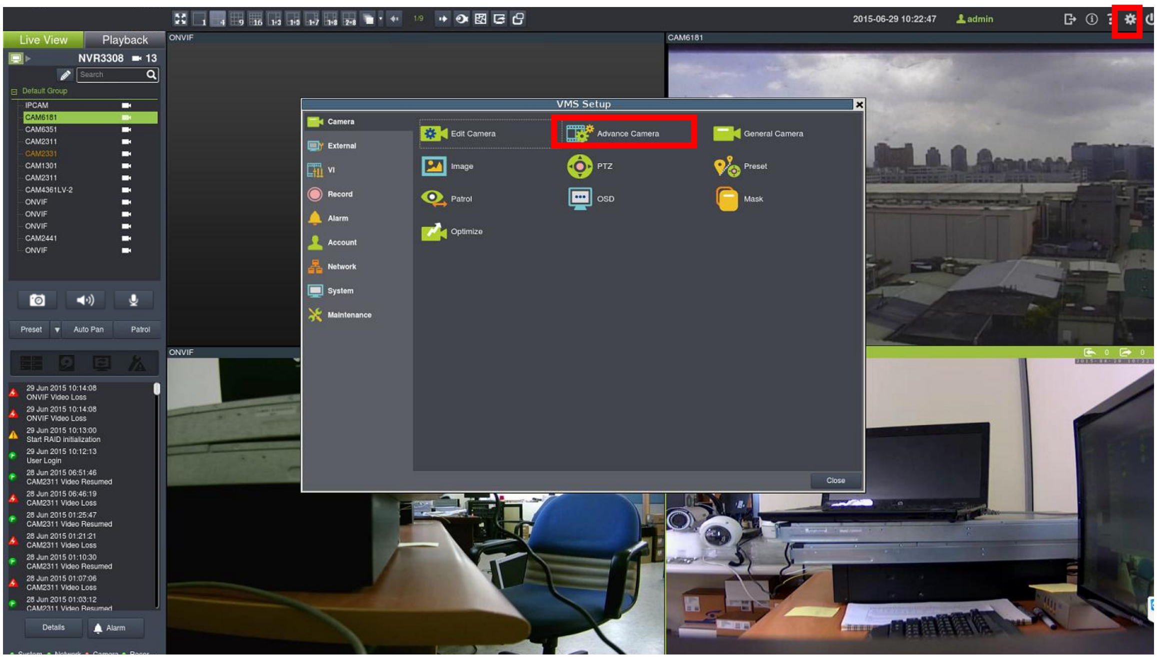
- □ IPCAM-<172.30.10.70>
- □ CAM6181-<172.30.10.181>
- □ CAM6351-<172.30.10.250>
- □ CAM2311-<172.30.10.97>
- □ CAM2331-<172.30.10.104>
- □ CAM1301-<172.30.10.99>
- □ CAM2311-<172.30.10.70>
- □ CAM2441-<172.30.10.55>
- □ CAM4361LV-2-<172.30.10.93>
- □ ONVIF-<172.30.10.61>
- □ ONVIF-<172.30.10.66>
- □ ONVIF-<172.30.10.95>

8.3.2. Advanced Video Settings

1. Right-click the specific camera entry in the *Camera List below the Live View*, then click **Image > Advanced Video.**

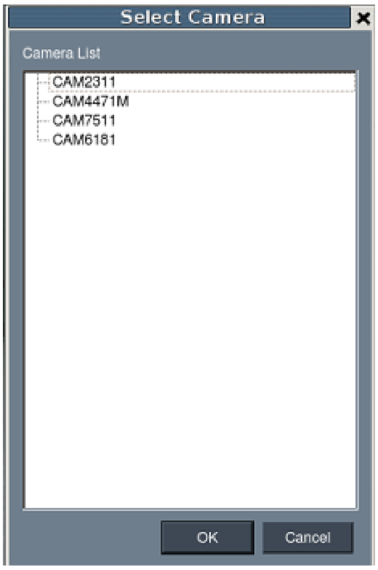


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Advanced Camera.**



```
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
28 Jun 2015 01:07:06
CAM2311 Video Loss
28 Jun 2015 01:03:12
CAM2311 Video Resumed
```

Select a specific camera for advanced camera settings.

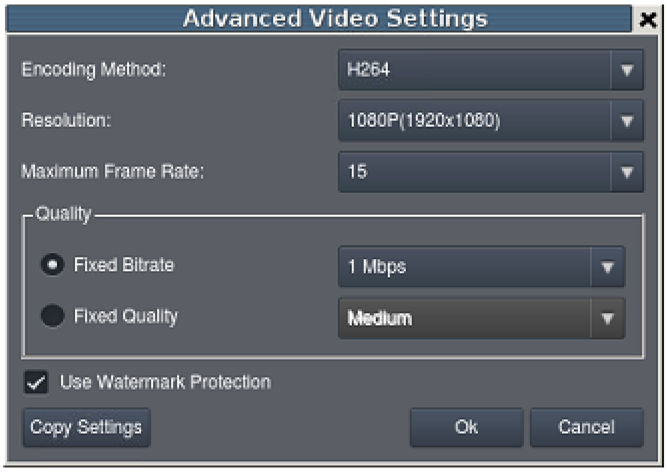


Select Camera

Camera List

- CAM2311
- CAM4471M
- CAM7511
- CAM6181

Note: You must be logged into the camera before changing settings or else the operation will fail.



Advanced Video Settings

Encoding Method:	H264
Resolution:	1080P(1920x1080)
Maximum Frame Rate:	15

Quality

◉ Fixed Bitrate	1 Mbps
○ Fixed Quality	Medium

☑ Use Watermark Protection

2. Select a video encoding method from the **Encoding Method** drop-down. Encoding methods will vary by camera type, but common ones include:
   - **MJPEG**
   - **H264**

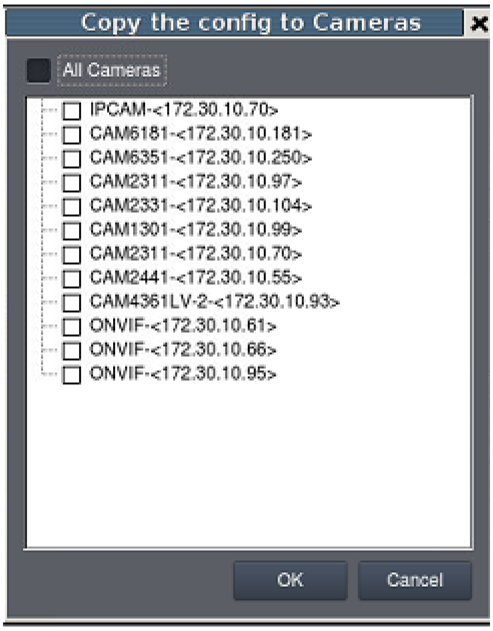
3. Select a video resolution from the **Resolution** drop-down. Supported resolutions will vary by camera.

4. Select the Select the maximum video frame rate from the **Maximum Frame Rate** drop-down.

5. From the *Quality* section, choose one of the following:

- **Fixed Bitrate** – The camera image quality will be adjusted within a fixed bitrate selected in the dropdown. Dropdown values will vary by camera.
- **Fixed Quality** – The camera bitrate will be adjusted to meet the quality selected in the dropdown. Dropdown values will vary by camera.

6. Click **Copy Settings** to have the same settings applied to other cameras. Once **Copy Settings** button is clicked, the following window will appear. Select the cameras you'd like to have the same settings applied to save time.



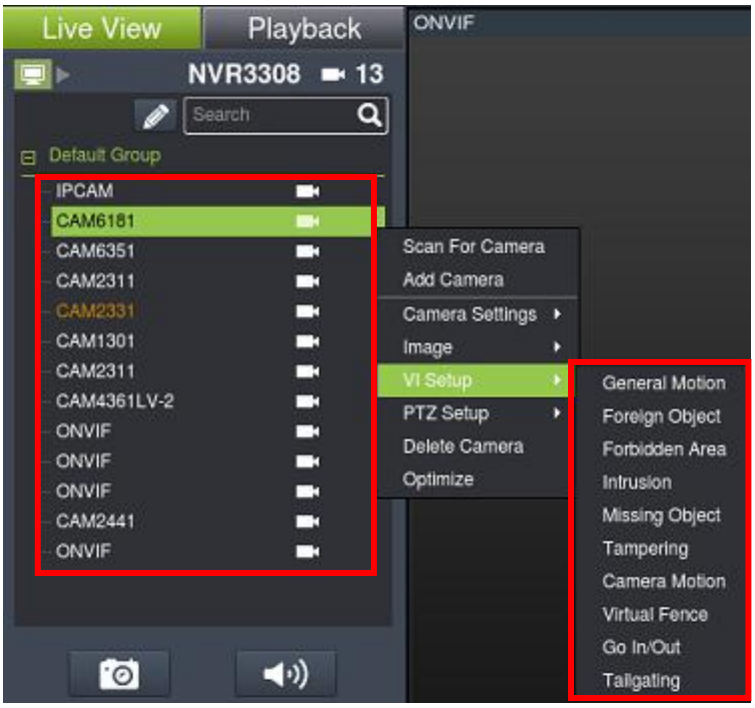
Copy the config to Cameras

□ All Cameras

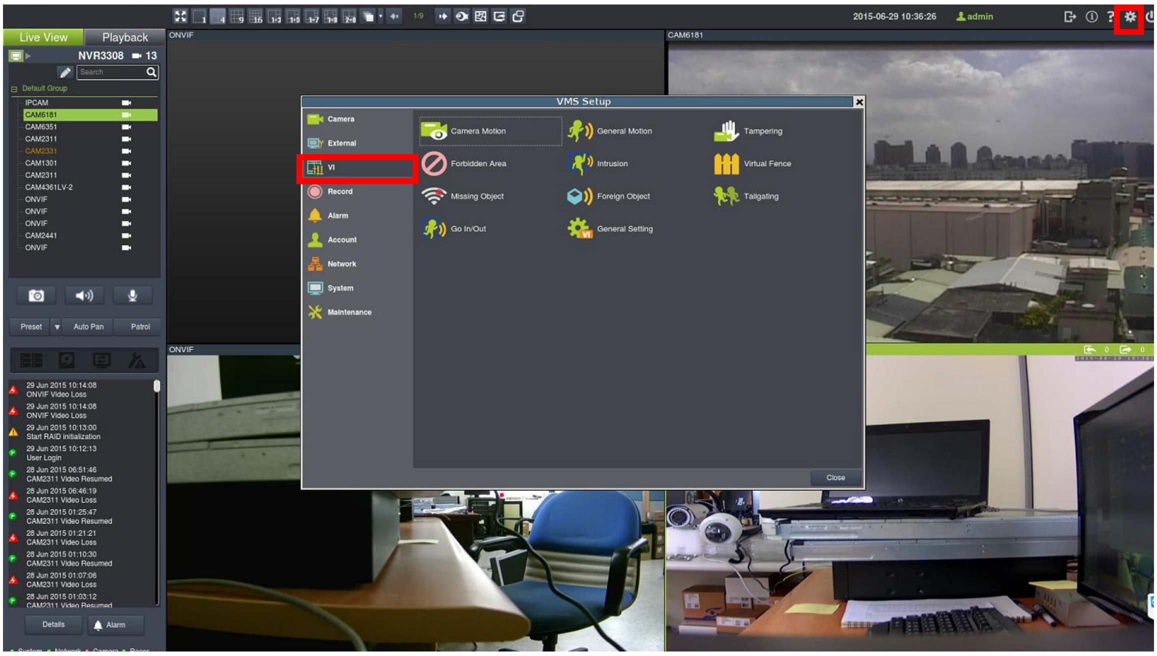
- □ IPCAM-<172.30.10.70>
- □ CAM6181-<172.30.10.181>
- □ CAM6351-<172.30.10.250>
- □ CAM2311-<172.30.10.97>
- □ CAM2331-<172.30.10.104>
- □ CAM1301-<172.30.10.99>
- □ CAM2311-<172.30.10.70>
- □ CAM2441-<172.30.10.55>
- □ CAM4361LV-2-<172.30.10.93>
- □ ONVIF-<172.30.10.61>
- □ ONVIF-<172.30.10.66>
- □ ONVIF-<172.30.10.95>

8.4. VI Setup

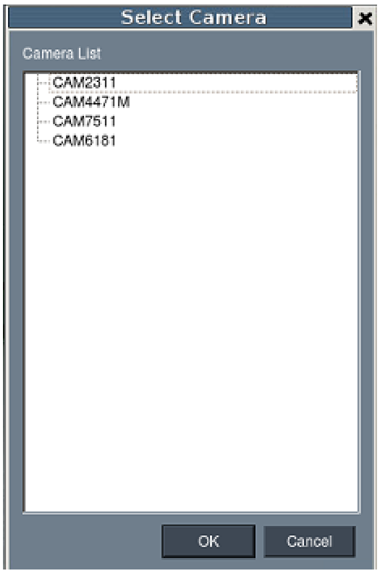
1. Right-click the specific camera entry in the *Camera List below the Live View*, then click **VI Setup**.



Or click ⚙ to bring out **VMS Setup** window and select **VI.**



Select a specific camera for VI Setup.

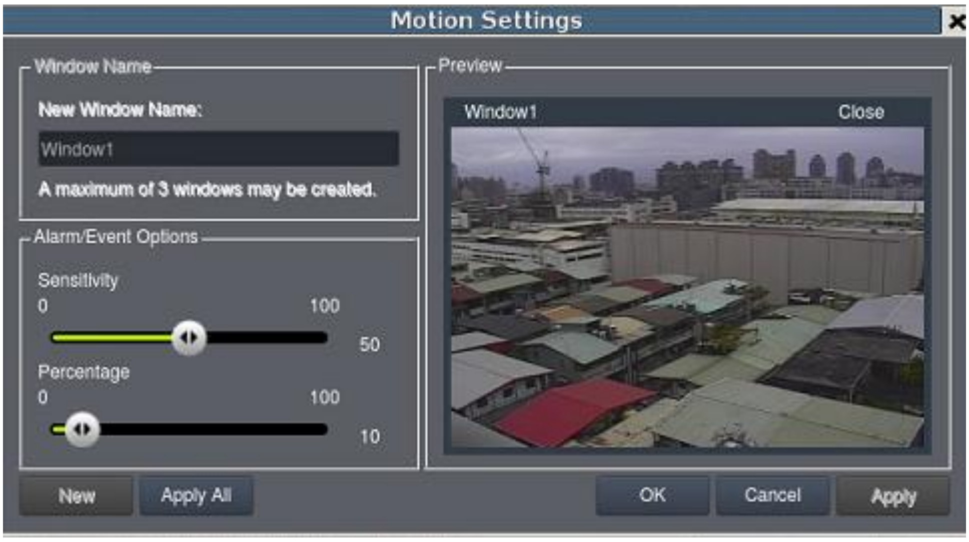

Select Camera

Camera List

- CAM2311
- CAM4471M
- CAM7511
- CAM6181

8.4.1. Camera Motion Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas.


Motion Settings

Window Name

New Window Name: Window1

A maximum of 3 windows may be created.

Alarm/Event Options

Sensitivity 0 100 50

Percentage 0 100 10

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Camera Motion Detection**.

> **Note:** You must be logged into the camera before changing settings or else the operation will fail.

2. If a new window is desired, enter a name in the **New Window Name** field and click the **New** button. Up to 3 detection windows can be set for each camera. The current window will be highlighted.

3. Click and drag the window border of a window to resize or reshape the window.

4. Click the interior of a window to drag it to the desired position.

5. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity -** Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Percentage -** Adjusts the amount of the window that must change before an event is triggered.

6. Click **Apply** to save the changes and **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

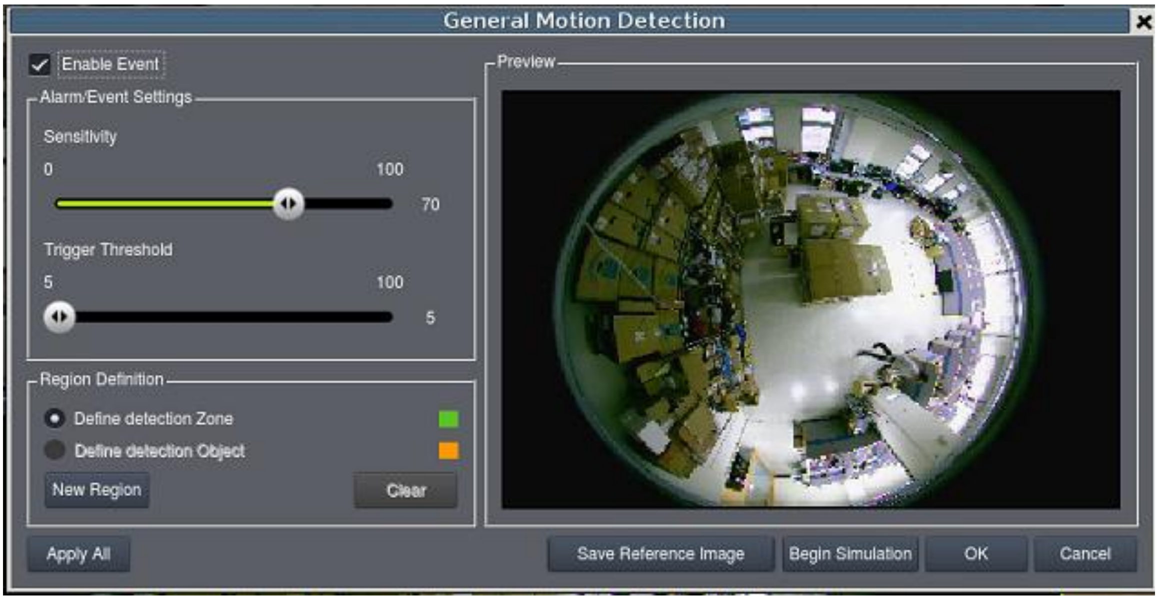
1. Right click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Camera Motion Detection** option.

2. Click the **X** at the top right corner of the window to delete the window.

3. Click **OK** to save the changes and exit the popup.

8.4.2. General Motion Detection

Automatically detect the moving target entering the security area. When it moves, an alarm will be triggered.



General Motion Detection

☑ Enable Event

Alarm/Event Settings

Sensitivity: 0–100, 70

Trigger Threshold: 5–100, 5

Region Definition

● Define detection Zone 🟩

○ Define detection Object 🟧

Enabling or Disabling a Detection

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > General Motion Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > General Motion Detection**.
2. If a new window is desired, click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a green border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. Adjust the sliders: (Settings will be applied to all existing windows)

- **Sensitivity** – Adjusts window sensitivity from 0 (low) to 100 (high).
- **Trigger Threshold -** Adjusts the amount of change allowed before and event is triggered.

6. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

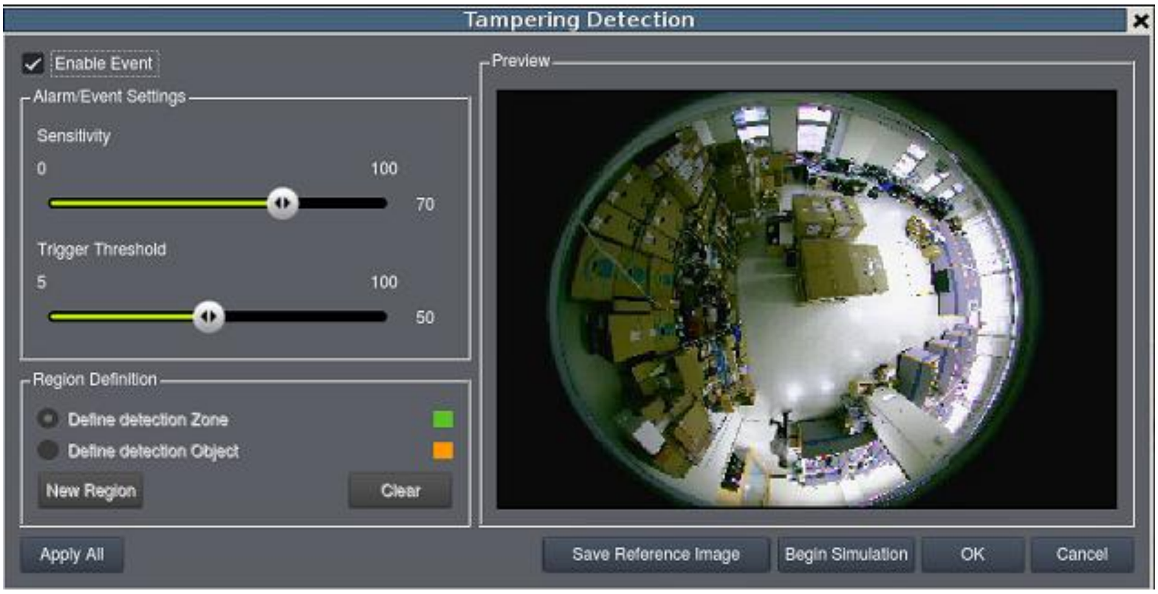
1. Right-click the camera entry in the *list of the Live View*, then highlight and click the **VI Setup > General Motion Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any moving objects detected.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > General Motion Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.3. Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected.



Tampering Detection

☑ Enable Event

Alarm/Event Settings

Sensitivity (0–100): 70

Trigger Threshold (5–100): 50

Region Definition

○ Define detection Zone 🟩

○ Define detection Object 🟧

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Tampering Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring Tampering Detection

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Tampering Detection**.
2. Adjust the sliders:
   - **Sensitivity -** Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Trigger Threshold -** Adjusts the amount of change allowed before an event is triggered.
3. Click **OK** to save the changes and exit the popup.

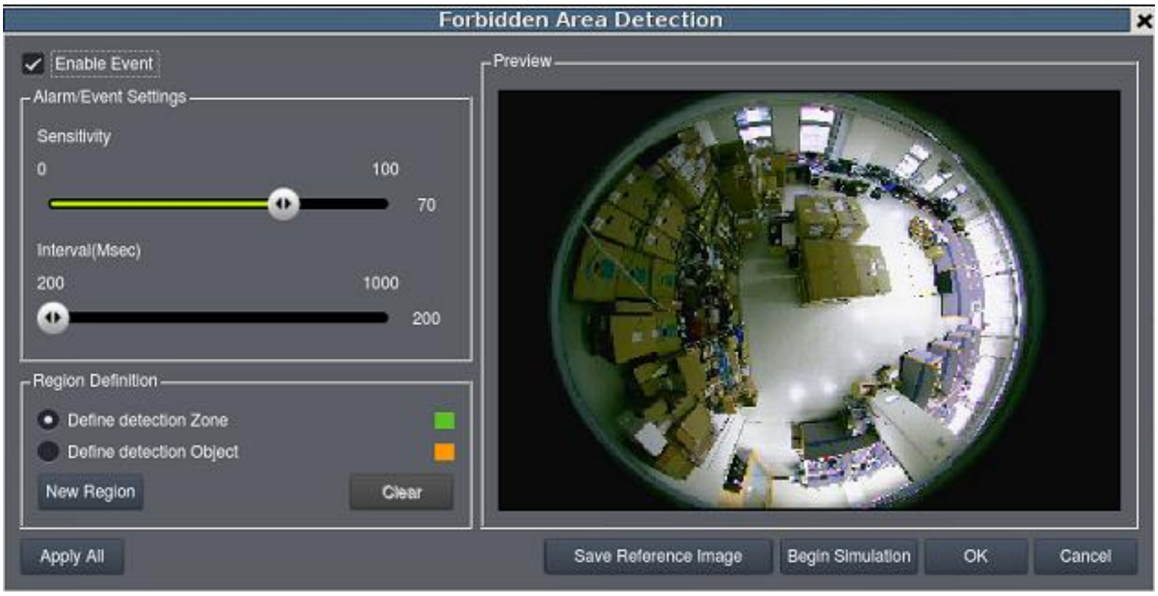
Testing Tampering Detection

To test a detection window:

- Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Tampering Detection** option.
- Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
- Click the **Begin Simulation** button enable test detection. During testing a red border if tampering is detected.
- Click **End Simulation** to end the simulation.
- Click **OK** to exit the popup.

8.4.4. Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas.



Forbidden Area Detection

☑ Enable Event

Alarm/Event Settings

Sensitivity: 0 – 100: 70

Interval(Msec): 200 – 1000: 200

Region Definition

● Define detection Zone 🟩

○ Define detection Object 🟧

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup** > **Forbidden Area Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup** > **Forbidden Area Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.

5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
   - **Sensitivity –** Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Interval -** Adjusts how much time between each check of the forbidden area.
8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Forbidden Area Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any objects detected in the forbidden area.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

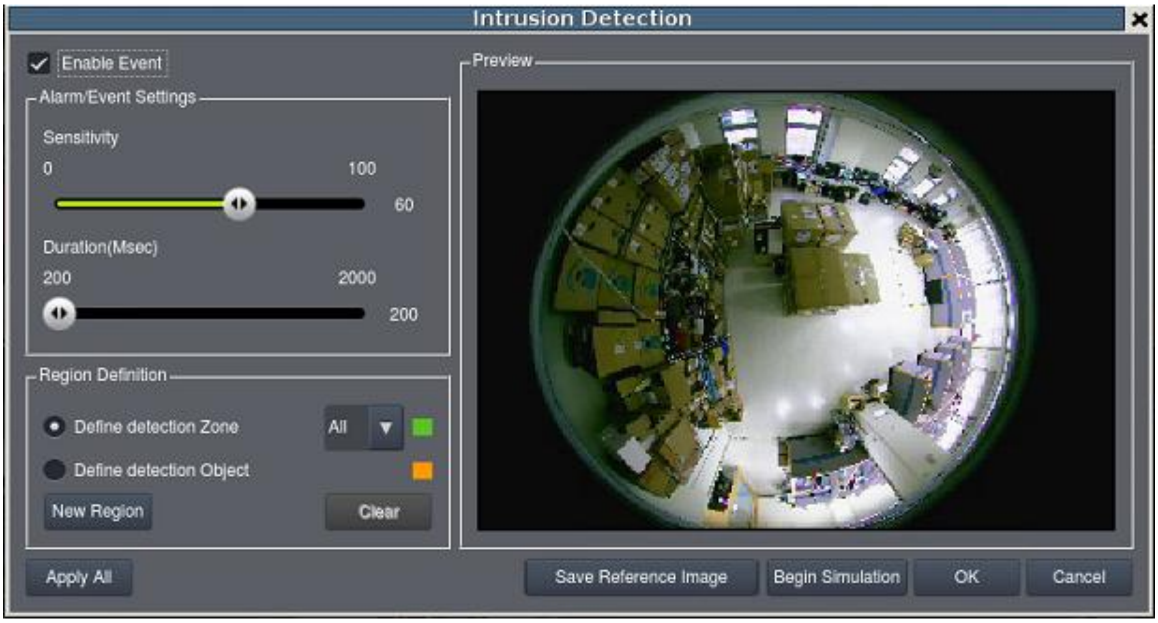
Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Forbidden Area Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.5 Intrusion Detection

Intrusion detection involves using the software to analyze the video feed and detect intrusion larger than a certain size.



Intrusion Detection

☑ Enable Event

Alarm/Event Settings

Sensitivity 0 100 60

Duration(Msec) 200 2000 200

Region Definition

● Define detection Zone All ▼ 🟩

○ Define detection Object 🟧

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Intrusion Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Intrusion Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.

5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the intrusion that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity -** Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Duration (Sec)** - Adjusts how much time an object is missing before an event is triggered.

8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Camera List below the Live View, then highlight and click the **VI Setup > Intrusion Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

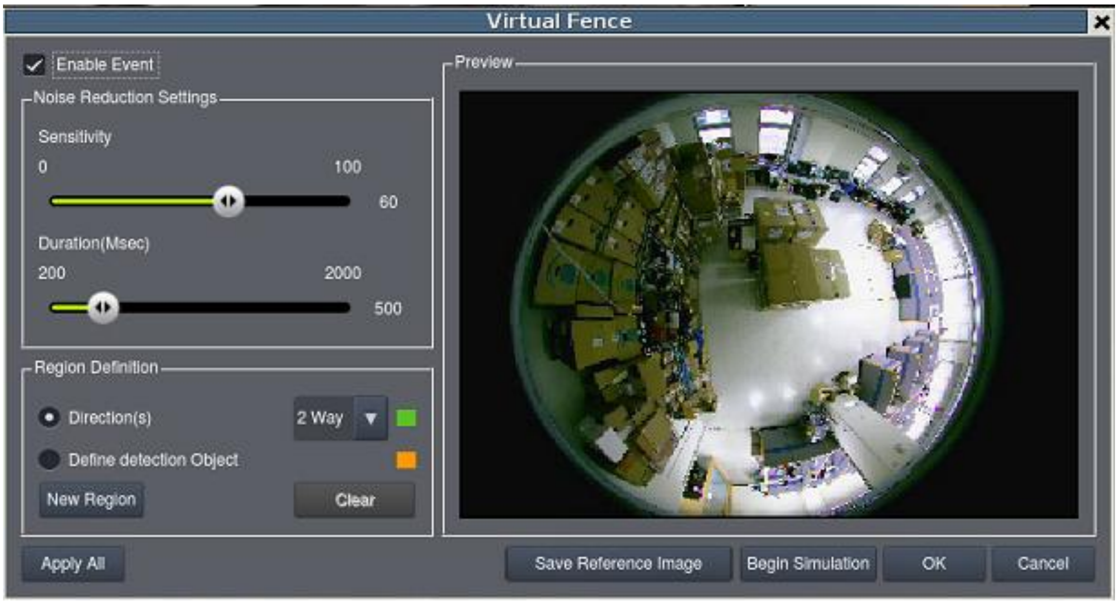
Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Intrusion Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.6. Virtual Fence

Virtual fence involves using the software to create a fence-crossing detection of the demanding object.



Virtual Fence

☑ Enable Event

Noise Reduction Settings

Sensitivity 0 100: 60

Duration(Msec) 200 2000: 500

Region Definition

● Direction(s) 2 Way 🟩

○ Define detection Object 🟧

Enabling or Disabling a Detection

To enable or disable the detection functions:

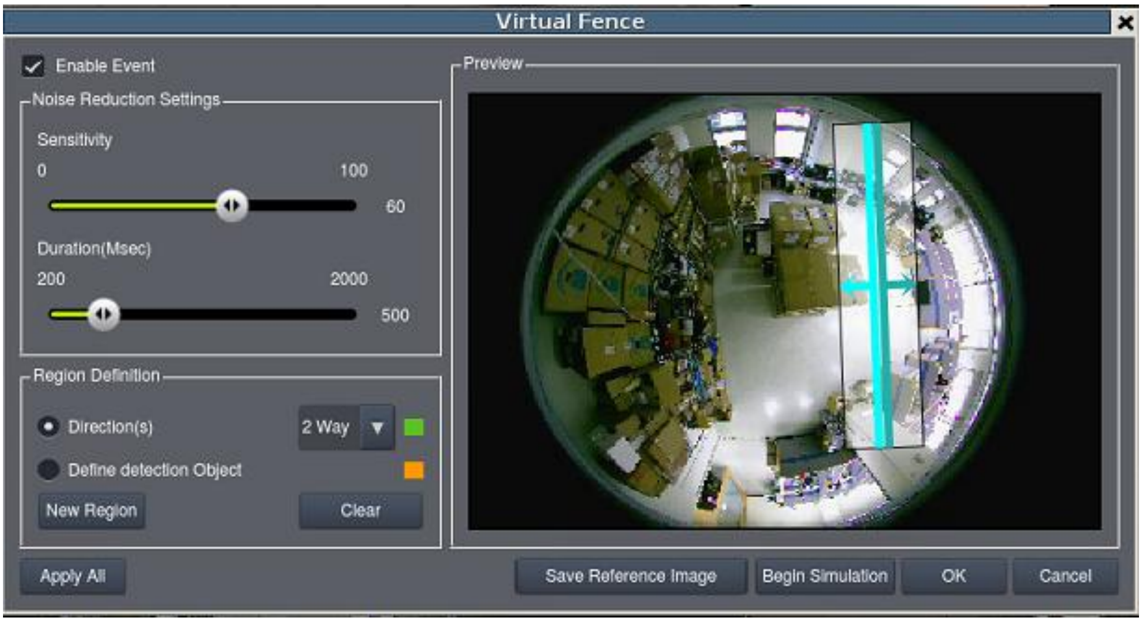
1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup** > **Virtual Fence** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup** > **Virtual Fence**.

   If a new window is desired, select **Directions** and click the **New Region** button to create a new window. The current window will be highlighted with a one/two-way arrow (blue means “in”, green means out”)



Virtual Fence

☑ Enable Event

Noise Reduction Settings

Sensitivity 0 100 60

Duration(Msec) 200 2000 500

Region Definition

● Direction(s) 2 Way 🟩

○ Define detection Object 🟧

2. Click and drag the white arrows along the window border around the one/two-way arrow to resize the space between the fences/adjust the length of the fences.

3. Turn the window border with the orange arrow to change the directions of the fences.

4. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.

5. Click and drag the corners of the object box to define the minimum size of the fence-crossing objects that will be detected.

6. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity – Adjusts window sensitivity from 0 (low) to 100 (high).**
   - **Duration (Sec)** - Adjusts how much time between each check for the fence-crossing.

7. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Camera List below the Live View, then highlight and click the **VI Setup > Virtual Fence** option.

2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if a object goes missing.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

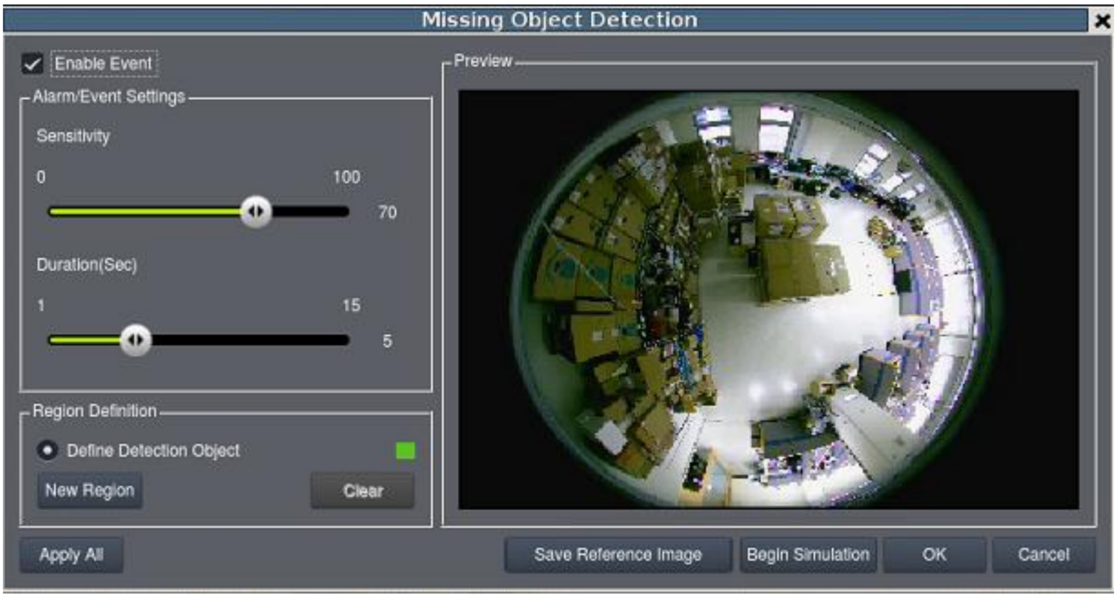
Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Virtual Fence** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.7. Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size.



Missing Object Detection

☑ Enable Event

Alarm/Event Settings

Sensitivity

0 100

70

Duration(Sec)

1 15

5

Region Definition

● Define Detection Object 🟩

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Missing Object Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Missing Object Detection.**
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.

4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the missing objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity - Adjusts window sensitivity from 0 (low) to 100 (high).**
   - **Duration (Sec)** - Adjusts how much time an object is missing before an event is triggered.

8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Camera List below the Live View, then highlight and click the **VI Setup > Missing Object Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a border will appear if a object goes missing.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

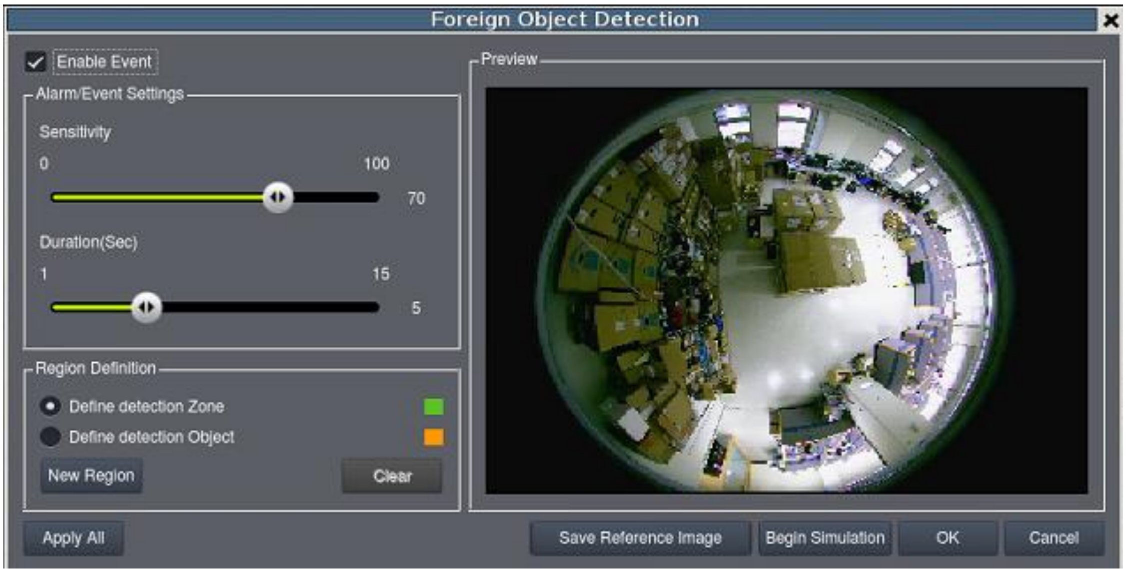
Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Missing Object Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

8.4.8. Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong.



Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Foreign Object Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click OK to save the changes and exit the popup.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, and click **VI Setup > Foreign Object Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.

4. Click the interior of a window to drag it to the desired position.

5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.

6. Click and drag the corners of the object box to define the minimum size of objects that will be detected.

7. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity -** Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Duration** - Adjusts the amount of time before an object triggers an event.

Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Foreign Object Detection** option.
2. Click **Save Reference Image** to have a reference image saved and the system will use this saved image to compare with the live recording image to see if there is any different; when the 2 images are different, the alarm will be triggered.
3. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any foreign objects detected.
4. Click **End Simulation** to end the simulation.
5. Click **OK** to exit the popup.

Deleting a Detection Window

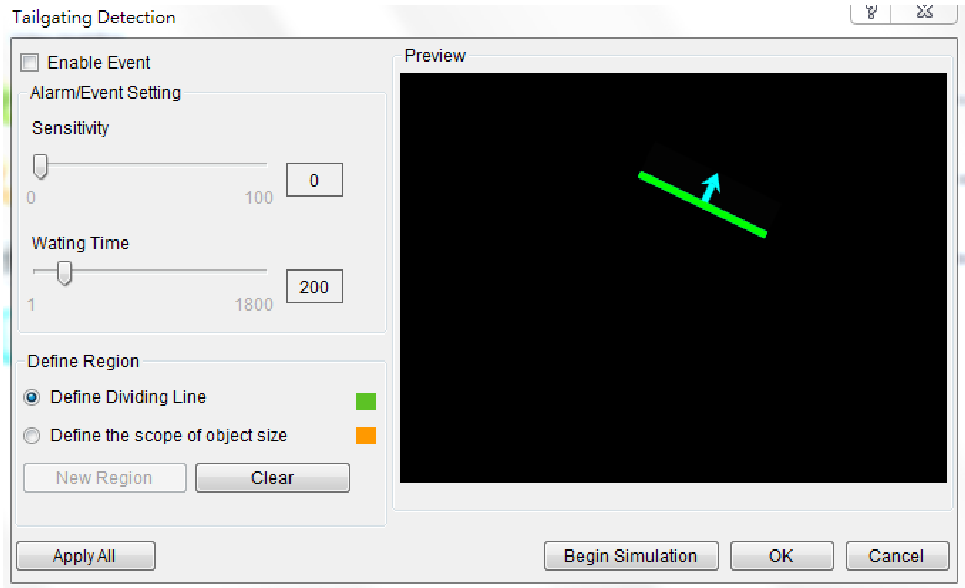
To delete a new detection window:

1. Right-click the camera entry in the *Camera List below the Live View*, then highlight and click the **VI Setup > Foreign Object Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.

8.4.9. Tailgating Detection

This functionality is currently available for remote client only.

Tailgating detection involves using the software to analyze the video feed and detect a tailgating object crossing over the restricted area.



Tailgating Detection

☐ Enable Event

Sensitivity: 0

Wating Time: 200

● Define Dividing Line 🟩

○ Define the scope of object size 🟧

Note: Tailgating Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Tailgating Detection*** in the VMS Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Setup** > **Tailgating Detection**.
2. If a new window is desired, select Define Dividing Line and click the New Region button to create a new dividing line. Only 1 dividing line can be set for each camera.
3. Click and drag the created dividing line to the desire position and direction.
4. If an object size has not yet been defined, select Define Object and click the New Region button to create an object box.
5. Click and drag the corners of the object box to define the minimum size of the objects that will be detected.
6. Adjust the sliders: (Settings will be applied to all existing windows)

- Sensitivity – Adjusts window sensitivity from 0 (low) to 100 (high).
- Waiting Time (Sec) - Adjusts how much time an object is tailgating before an event is triggered.

7. Click OK to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Setup > Tailgating Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Dividing Line

To delete a new dividing line:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Tailgating Detection** option.
2. Highlight the dividing line.
3. Click the **Clear** button to delete the line.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

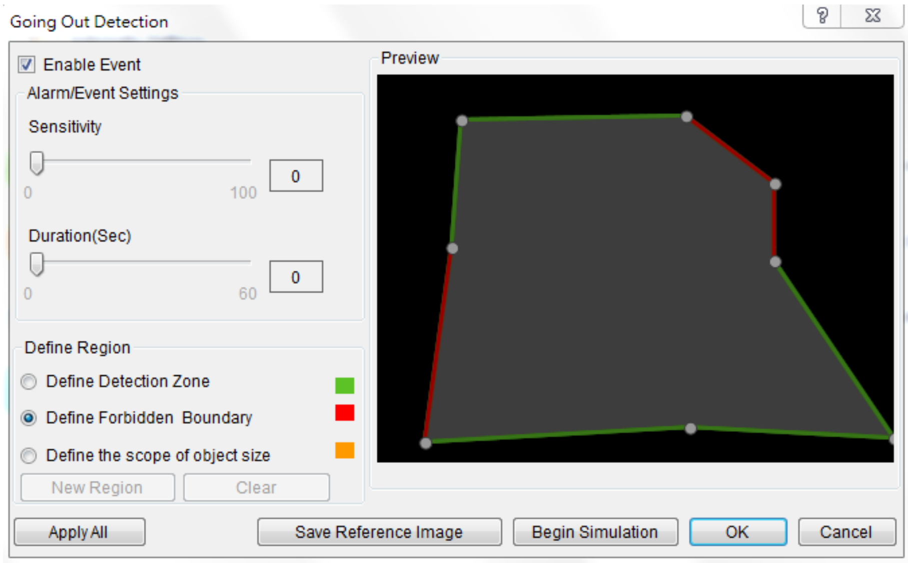
To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Tailgating Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

8.4.10. Go In/Out Detection

This functionality is currently available for remote client only.

Go in/out detection involves using the software to analyze the video feed and detect a go in/out object crossing over the restricted area.


Going Out Detection

☑ Enable Event

Alarm/Event Settings

Sensitivity: 0 (0–100)

Duration(Sec): 0 (0–60)

Define Region

○ Define Detection Zone 🟩

● Define Forbidden Boundary 🟥

○ Define the scope of object size 🟧

> **Note:** Go In/Out Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Go In/Out Detection*** in the VMS Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Setup** > **Go In/Out Detection**.
2. If a new window is desired, select Define Detection Zone and click the New Region button to create a new window. Only 1 detection window can be set for each camera.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to mark the restricted line; once clicked, the clicked line will turn red. The red lines are the boundaries. Up to 8 boundaries can be set.
5. If an object size has not yet been defined, select Define Object and click the New Region button to create an object box.

6. Click and drag the corners of the object box to define the minimum size of the objects that will be detected.

7. Adjust the sliders: (Settings will be applied to all existing windows)

   - Sensitivity – Adjusts window sensitivity from 0 (low) to 100 (high).
   - Duration (Sec) - Adjusts how much time an object is missing before an event is triggered.

8. Click OK to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Setup > Go In/Out Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Go In/Out Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Setup > Go In/Out Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.

8.5. PTZ Settings

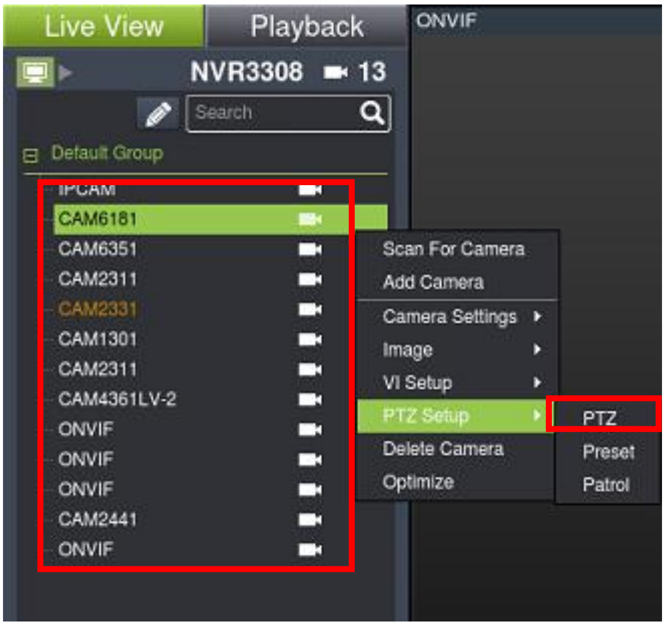
In cameras equipped with any combination of pan, tilt or zoom (PTZ) functionality, these settings are used to configure the PTZ functions.

8.5.1. PTZ Settings

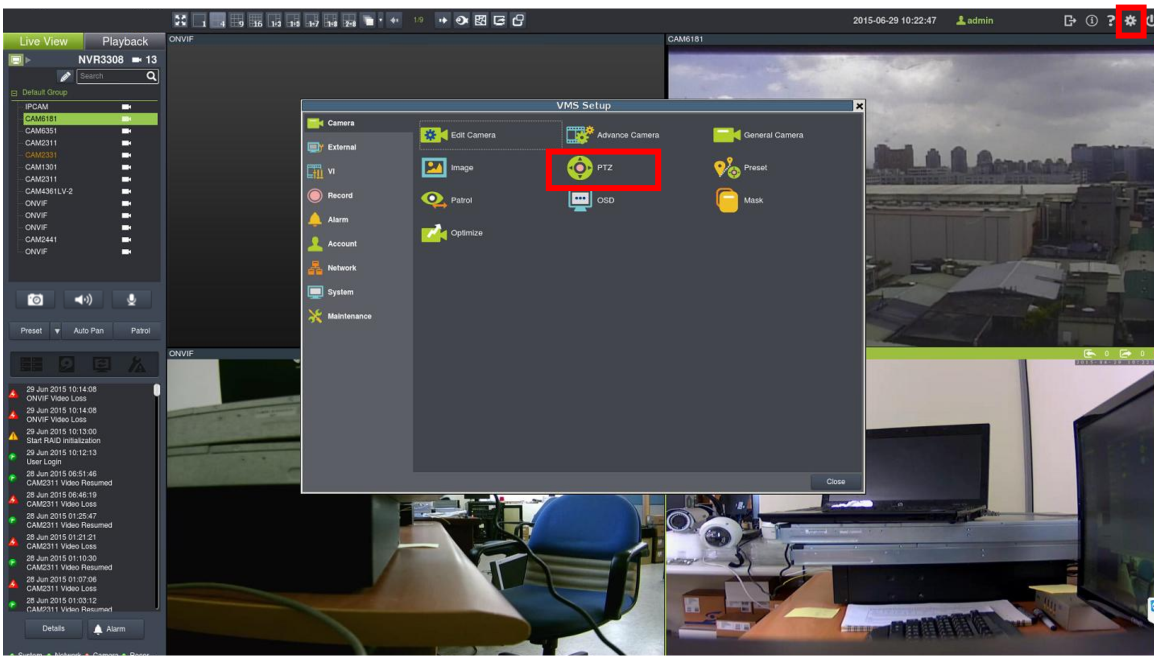
The PTZ settings deal with the software PTZ control panel. These settings adjust how much the camera will pan, tilt, zoom, and focus with each control panel input.

> **Note:** You must be logged into the camera before changing settings or else the operation will fail.

1. Right-click the specific camera with the PTZ functionality and click **PTZ Setup** > **PTZ**.

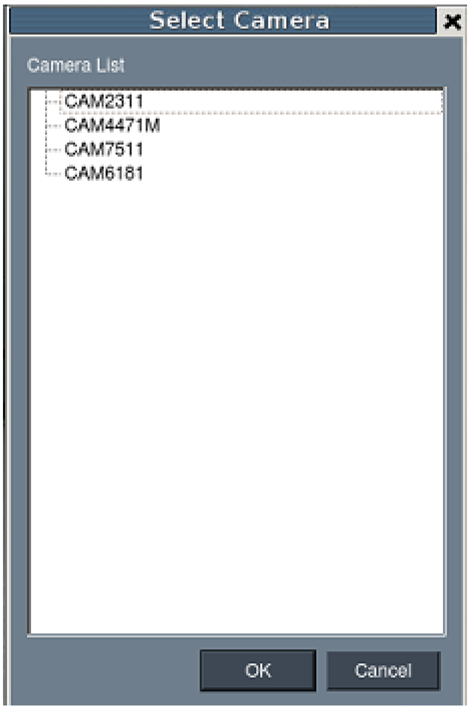


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **PTZ.**



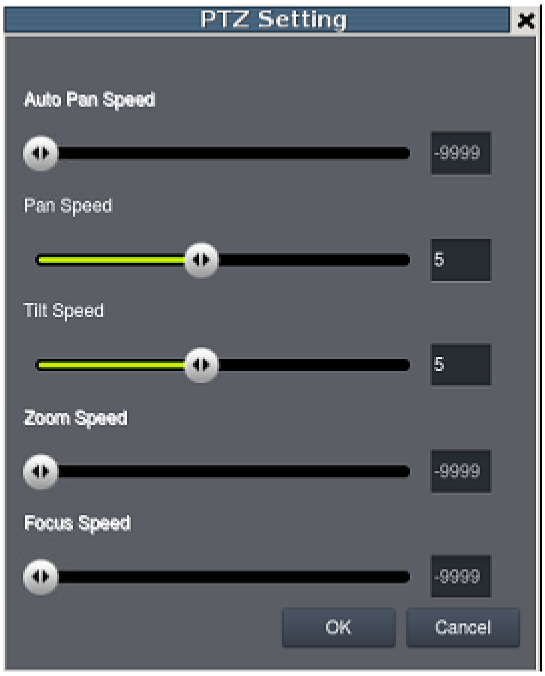
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
28 Jun 2015 01:07:06
CAM2311 Video Loss
28 Jun 2015 01:03:12
CAM2311 Video Resumed

Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.

2. Adjust the following sliders to increase and decrease the following speeds: (The higher the value, the higher the speed) Unsupported features on specific cameras will be grayed out.



Auto Pan Speed -9999

Pan Speed 5

Tilt Speed 5

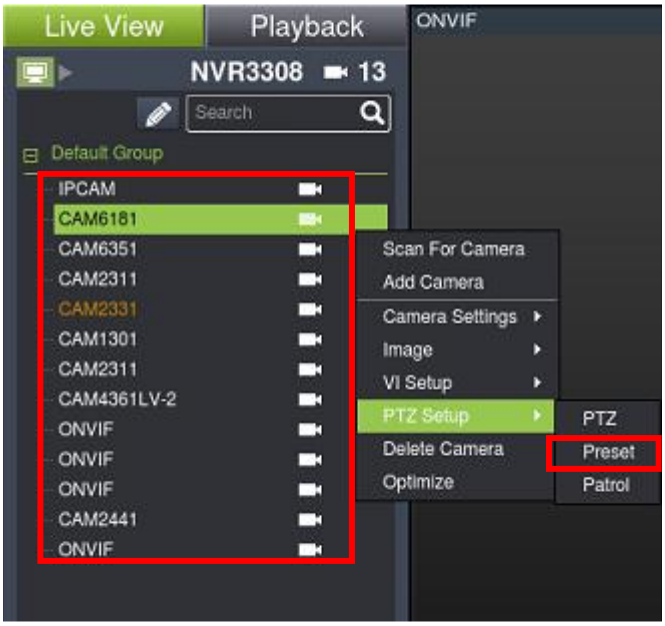
Zoom Speed -9999

Focus Speed -9999

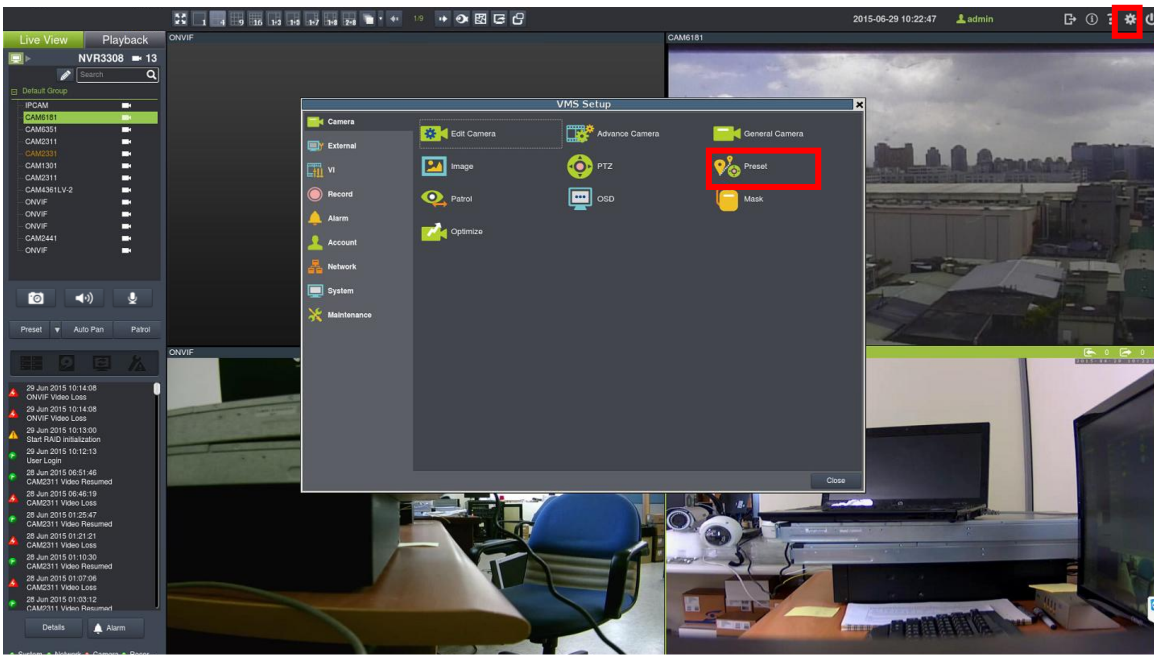
- **Auto Pan Speed** – The speed which the camera will pan between the mechanical stops when the **Auto Pan** function is activated.
- **Pan Speed** – The distance the camera will pan to each side.
- **Tilt Speed -** The distance the camera will tilt up and down.
- **Zoom Speed -** The distance the camera will zoom near or far.
- **Focus Speed -** The amount the camera will focus forward or backward.

8.5.2. PTZ Preset Settings

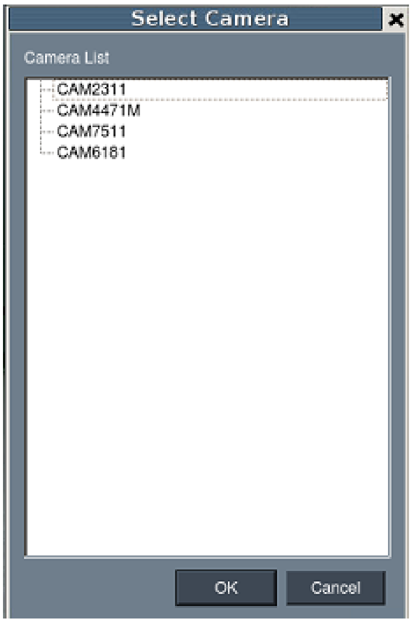
Certain preset pan/tilt/zoom values can be saved in order to move the camera quickly to a point of interest. To configure camera PTZ preset settings, right-click the specific camera with the PTZ functionality, then highlight and click **PTZ Setup > Preset** option.



Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Preset.**

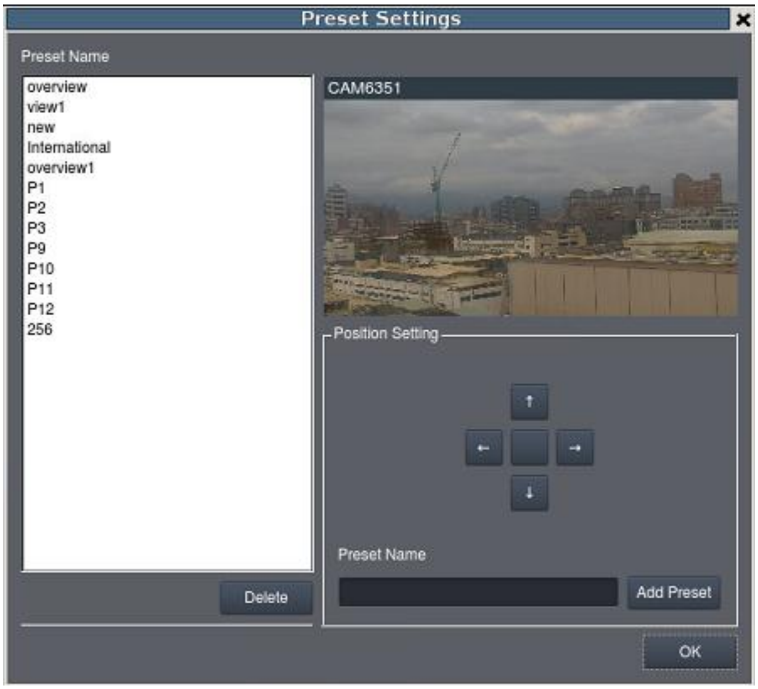


Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.

The popup will display the camera output, as well as a *Position Setting* pad.



Note: You must be logged into the camera before changing settings or else the operation will fail.

Adding a Preset

1. Use the directional pad to move the camera view. Use the center “home” button to return the camera to the default zeroed view.
2. Once the camera reaches the point where a preset is desired, type a name into the **Preset Point Name** field.
3. Click the **Add a preset point** to add the preset to the list. Click **OK** exit the menu, or you may continue to add/delete additional presets.

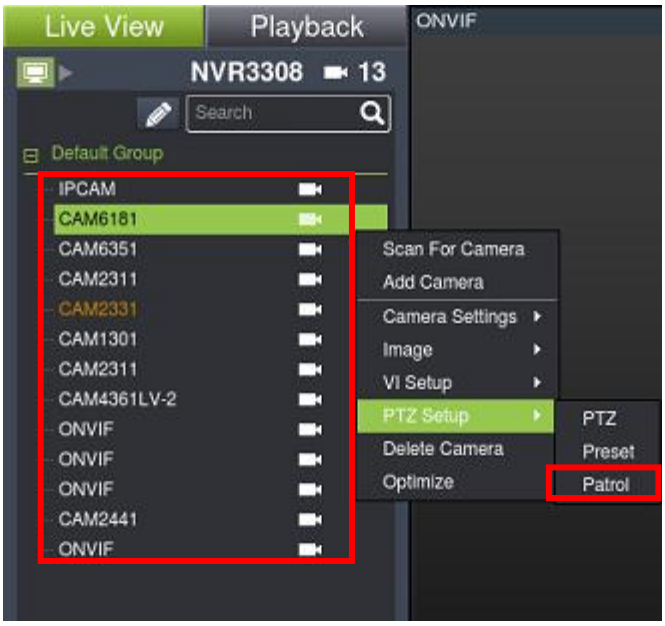
Deleting a Preset

To delete a preset, simpy highlight the preset and click the **Delete** button. Click the **Yes** button to confirm deletion. Click **OK** exit the menu, or you may continue to add/delete additional presets.

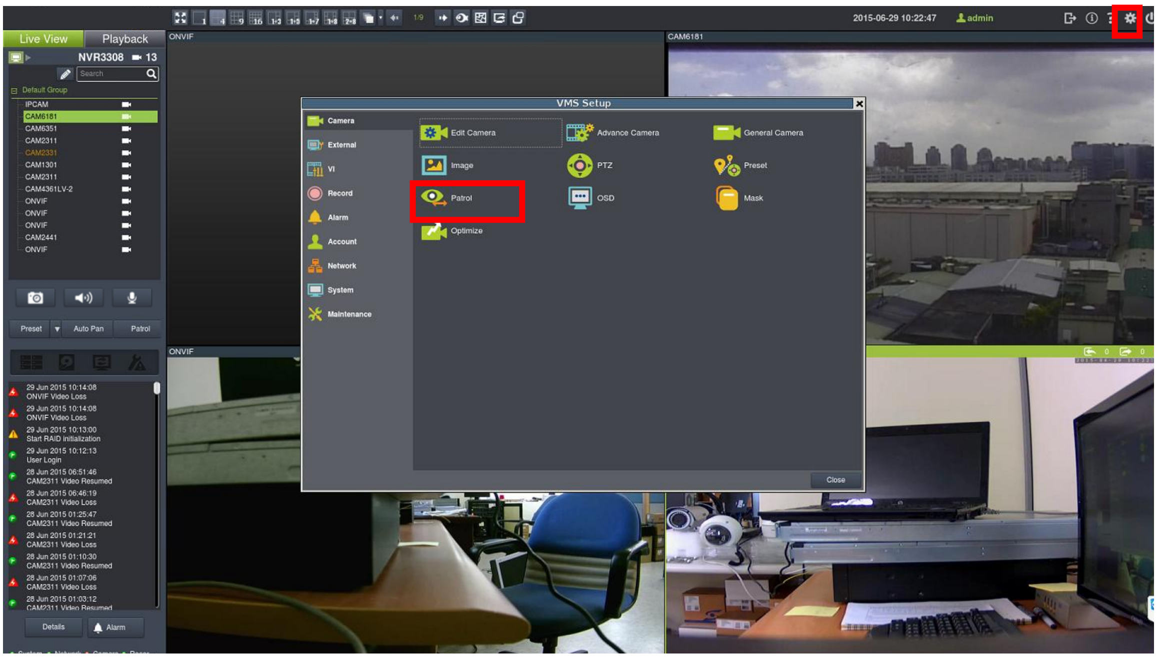
8.5.3. PTZ Patrol Settings

In cameras with PTZ functionality, one camera can be used to survey a large area. This can be done automatically using the patrol functionality. This function basically moves the camera between preset points in a fixed pattern. To configure camera patrol settings:

1. Right-click the specific camera with the PTZ functionality, highlight and click the **PTZ Setup > Patrol.**

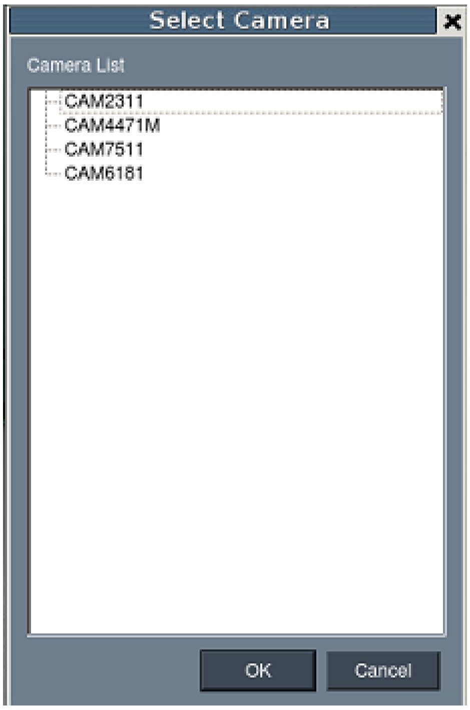


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Preset.**



Note: You must be logged into the camera before changing settings or else the operation will fail.

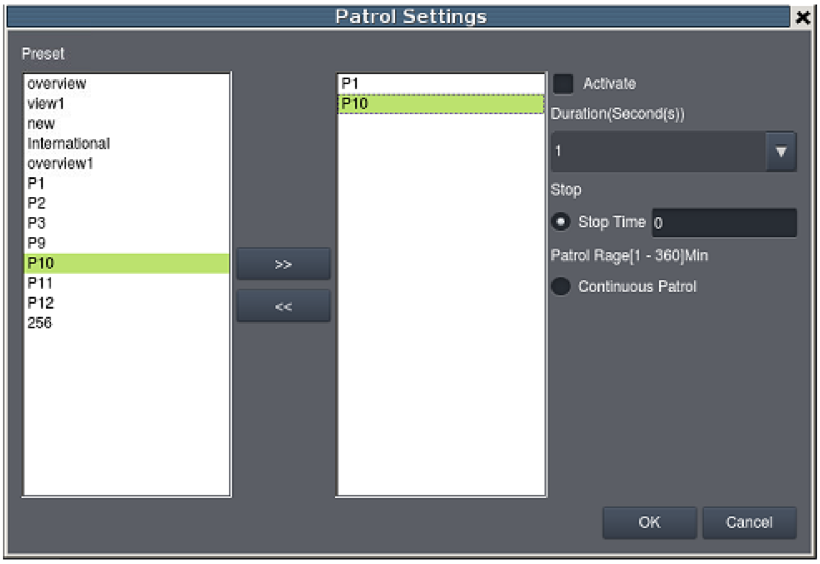
Select a specific camera for advanced camera settings.



Camera List

- CAM2311
- CAM4471M
- CAM7511
- CAM6181

Note: You must be logged into the camera before changing settings or else the operation will fail.



Preset

overview
view1
new
international
overview1
P1
P2
P3
P9
P10
P11
P12
256

P1
P10

□ Activate

Duration(Second(s)): 1 ▼

Stop

● Stop Time 0

Patrol Rage[1 - 360]Min

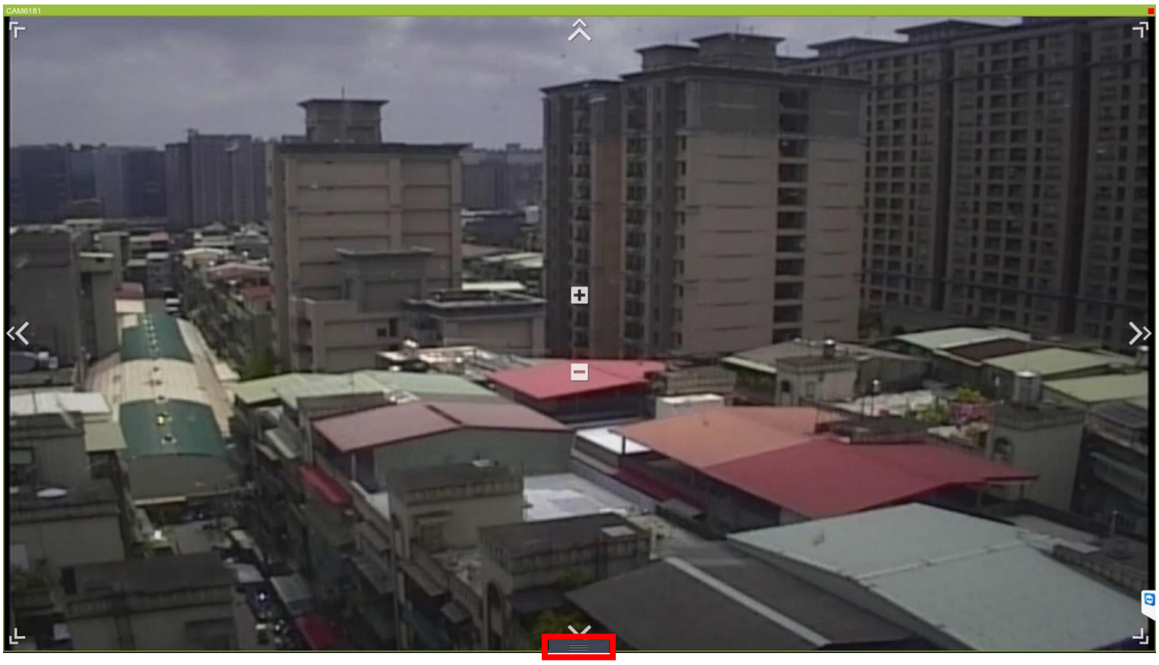
○ Continuous Patrol

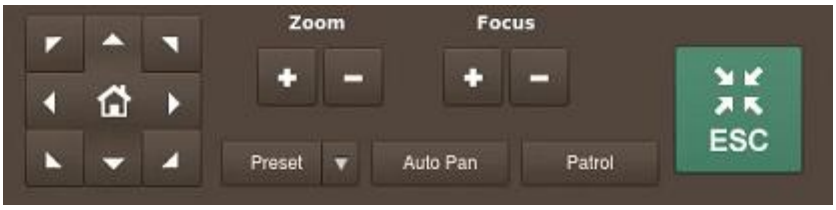
1. On the right side of the popup there will be a list of preset points that are defined for the camera. Use the **>>** button to add the points to the patrol list in the order that they are to be viewed. Points can also be removed by highlighting them and clicking on the **<<** button.
2. Select the length of time the camera will dwell at each preset point before continuing from the **Dwelling Time (Sec)** dropdown.
3. Select one of the following:
   - **Stop Time** – The camera will stop the number of minutes specified in the box between patrol sessions.
   - **Continuous Patrol** – The camera will not stop between patrol sessions.
4. Check the **Active box** to activate the patrol list.
5. Click the **OK** button to save the patrol list and exit the popup.

8.5.4. On-screen PTZ Controls

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the local client software. These controls can be seen in the live view screen.

Once your mouse hovers over the gray index marked by a red box below, you'll see a PTZ panel. Use the PTZ panel to perform PTZ related functionalities.





> **Note:** (1) The camera to be controlled must be selected by highlighting it (clicking its output window) in the main view window.

8.5.5. Directional Pad

Pan and Tilt

The pan and tilt functionalities can be controlled with the directional pad.

Clicking the right or left arrow will pan the camera by one step in the direction clicked. Clicking the up or down arrow will tilt the camera by one step in the direction clicked. Clicking diagonal arrows will combine the pan and tilt action of the adjacent arrows. Clicking on the Home icon, located at the center of the pad, will re-center the camera.

8.5.6. Functional Buttons

Home

One position can be set as the Home position. Click on Home button to go to the Home position. Clicking on the Home button will re-center the camera.

Preset

The camera may have preconfigured viewpoints, or presets configured. To switch to one of these presets, click the **Preset** button and select the preset.

Auto Pan

The camera will start or stop pan between the mechanical stops.

Patrol

In cameras with PTZ functionality, one camera can be used to survey a large area. This can be done automatically using the patrol functionality.

Zoom

The zoom on a camera can be controlled with the + and – buttons located inside the direction pad. Pressing the + button will increase zoom distance by 1 step. Pressing the - button will decrease zoom distance by one step.

Focus

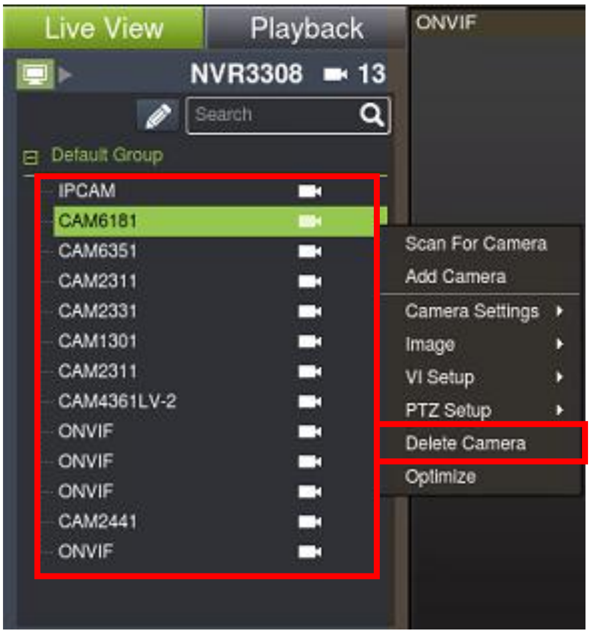
The focus on a camera can be controlled with the + and - buttons located beside the *Focus* box. Pressing the + button will increase focus distance by 1 step. Pressing the - button will decrease focus distance by one step.

ESC

Use ECS button to go back to the original view.

8.6. Deleting a Camera

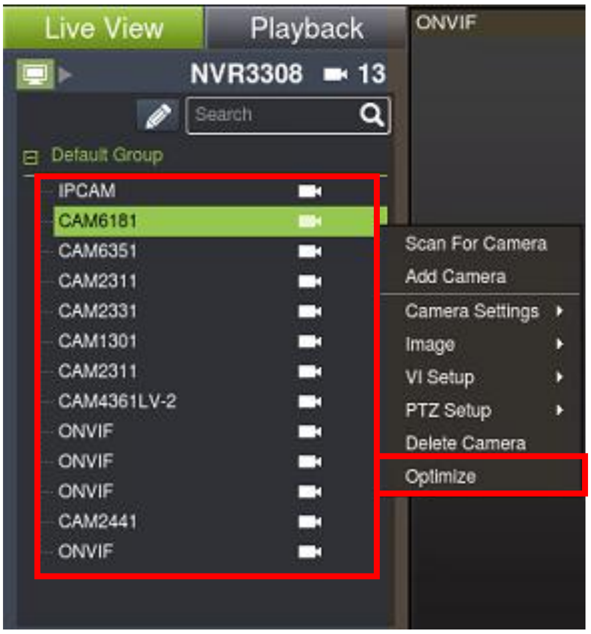
1. Right-click the camera entry you wish to remove to bring out the options popup. Highlight and click the **Delete Camera** option.



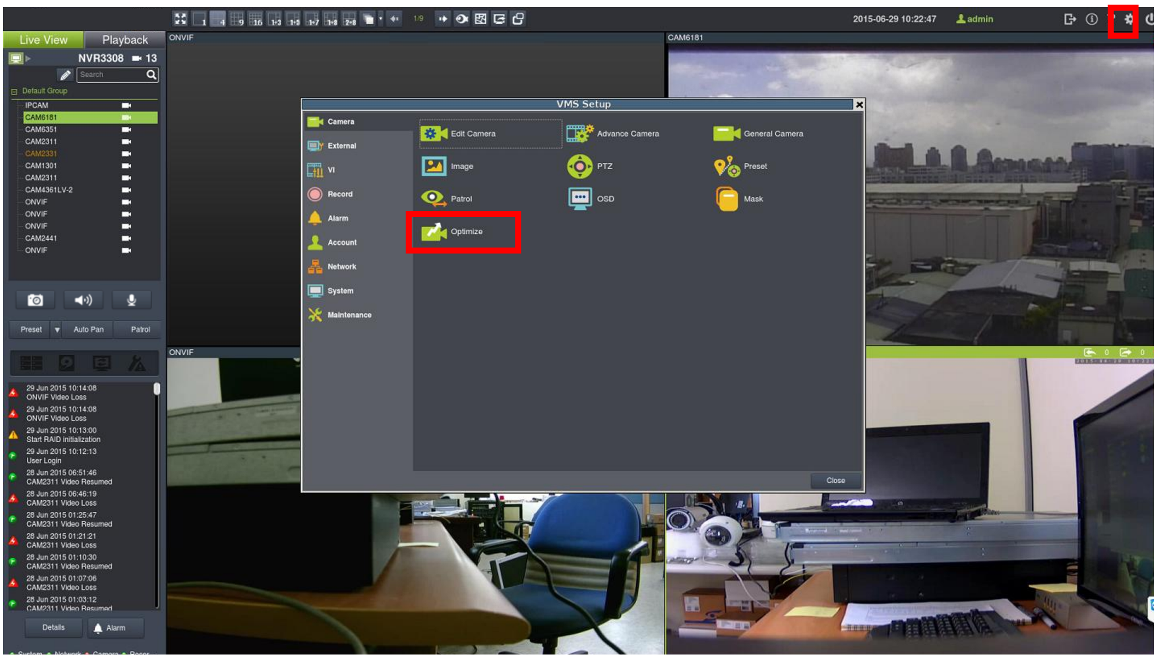
8.7. Optimizing a Camera

Optimizing the camera resets the camera so that it will correspond to the settings on the Server. To perform this operation:

1. Right-click the camera entry you wish to remove to bring out the options popup. Highlight and click the **Optimize** option.

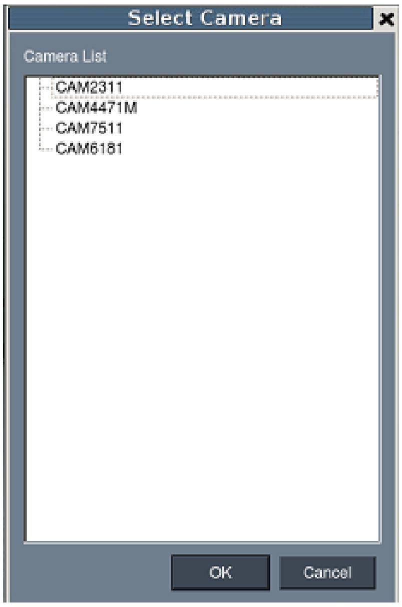


Or click ⚙ to bring out **VMS Setup** window and select **Camera** and then select **Optimize.**



29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
28 Jun 2015 01:07:06
CAM2311 Video Loss
28 Jun 2015 01:03:12
CAM2311 Video Resumed

Select a specific camera for advanced camera settings.



Note: You must be logged into the camera before changing settings or else the operation will fail.

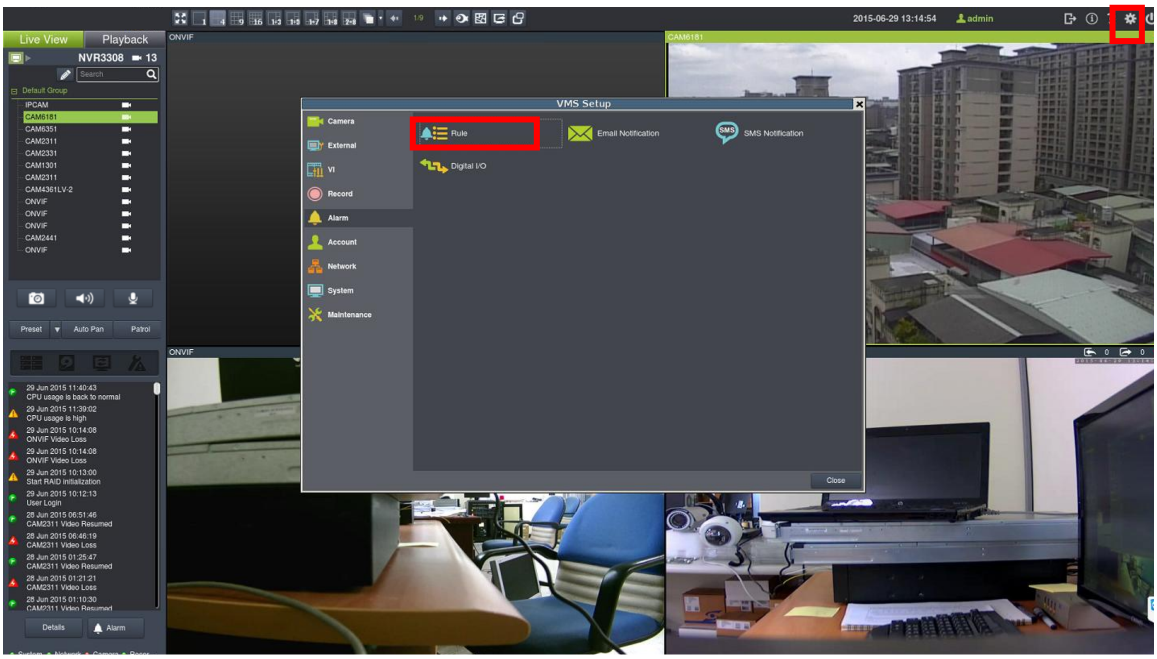
Chapter 9. Alarms and Events

This section will guide the user through the detection setup and digital Inputs for detecting alarm conditions, the setup of digital outputs and alarm popups and notifications, as well as the setup of alarm rules and schedules.

9.1. Alarm Rules

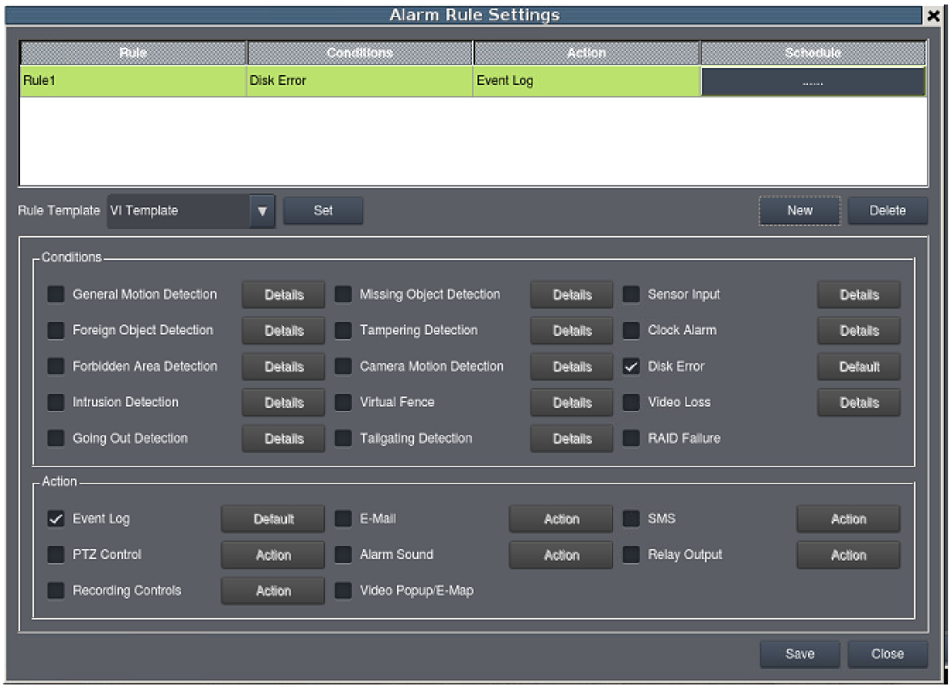
VMS Client provides robust alarm handling features.

To access these features click ⚙ to bring out **VMS Setup** window and select **Alarm** and then **Rules**.



29 Jun 2015 11:40:43
CPU usage is back to normal
29 Jun 2015 11:39:02
CPU usage is high
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed

In the Alarm Rules, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. Multiple alarm rules can be created using the following elements:



Rule	Conditions	Action	Schedule
Rule1	Disk Error	Event Log	......

Rule Template: VI Template

Conditions

☐ General Motion Detection ☐ Missing Object Detection ☐ Sensor Input
☐ Foreign Object Detection ☐ Tampering Detection ☐ Clock Alarm
☐ Forbidden Area Detection ☐ Camera Motion Detection ☑ Disk Error
☐ Intrusion Detection ☐ Virtual Fence ☐ Video Loss
☐ Going Out Detection ☐ Tailgating Detection ☐ RAID Failure

Action

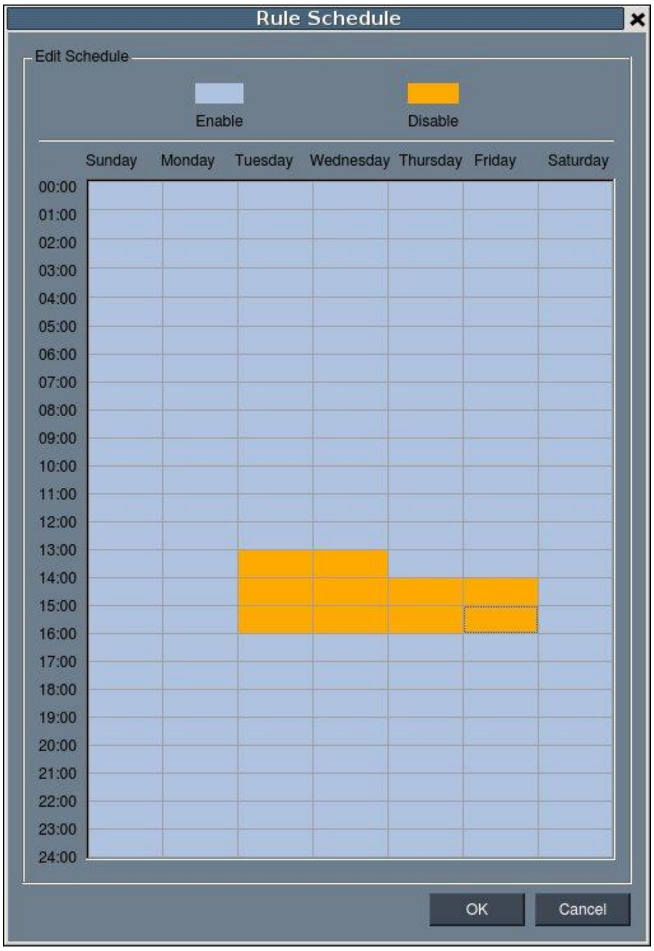
☑ Event Log ☐ E-Mail ☐ SMS
☐ PTZ Control ☐ Alarm Sound ☐ Relay Output
☐ Recording Controls ☐ Video Popup/E-Map

Alarm handling in the VMS is divided into **4** distinct phases:

1. **Rule**: An alarm rule combines conditions with corresponding actions.
2. **Condition**: The condition is the triggering event for the alarm such as Motion/Video loss/Sensor Input/Clock Alarm, etc.
3. **Action**: Specifies steps and actions that can be undertaken when an alarm is triggered.
4. **Schedule**: Allows the user to schedule the application of specific alarm rules. This is useful in cases such as applying rules to non-office hours.

9.1.1. Adding an Alarm Rule

1. Click the **New** button.
2. Enter a short description for the new rule in the **Add Rule** field.
3. Choose conditions and actions. Click the **......** button in the alarm field to set up a schedule for the rule. These selections are described in the following sections.



Rule Schedule

Edit Schedule

🟦 Enable   🟧 Disable

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
01:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
02:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
03:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
04:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
05:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
06:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
07:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
08:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
09:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
10:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
11:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
12:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
13:00	🟦	🟦	🟧	🟧	🟦	🟦	🟦
14:00	🟦	🟦	🟧	🟧	🟧	🟧	🟦
15:00	🟦	🟦	🟧	🟧	🟧	🟧	🟦
16:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
17:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
18:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
19:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
20:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
21:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
22:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
23:00	🟦	🟦	🟦	🟦	🟦	🟦	🟦
24:00							

4. Click the **Save** button to save the rule.

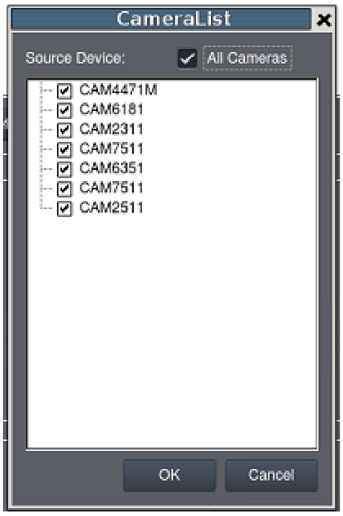
Conditions

The follow alarm conditions can be set to trigger the alarm:

When configuring a camera, a detection area can be specified for the following detections: General Motion Detection / Foreign Object Detection / Forbidden Area Detection / Intrusion Detection / Go In/Out Detection / Missing Object Detection / Tampering Detection / Camera Motion Detection / Virtual Fence / Tailgating Detection.

After the detection area is specified, detection can be activated and an alarm handling scheme configured in this menu.

Clicking on the **Detail** button will pull up a menu listing all the devices with General Motion Detection active.



Source Device: ☑ All Cameras

- ☑ CAM4471M
- ☑ CAM6181
- ☑ CAM2311
- ☑ CAM7511
- ☑ CAM6351
- ☑ CAM7511
- ☑ CAM2511

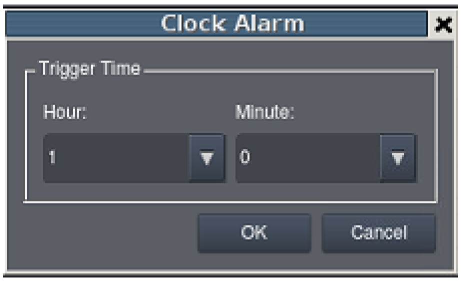
From this menu, click the checkboxes next to the cameras that have General Motion Detection configured. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

Sensor Input

The alarm is triggered by a sensor input. For example this may include doorway entry sensors that are connected to the camera system. Clicking on the Detail button will pull up the *Sensor Input Settings* menu, listing all the cameras. From this menu, click the checkboxes next to the cameras that will be used to trigger the Alarm. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

Clock Alarm

When a preset time is reached, the alarm is triggered. The Clock Alarm is triggered only on the day it is configured. Clicking on the **Detail** button will pull up the *Clock Alarm* menu.



Hour: 1

Minute: 0

From this popup select the hour and minute the alarm will be triggered. Click the **OK** button to exit the menu.

Disk Error

The alarm is triggered when a disk drive failure occurs.

Video Loss

When video input is lost, the alarm is triggered. Clicking on the **Details** button will pull up the *Video Loss Settings* menu, listing all the cameras. From this menu, click the checkboxes next to the cameras that will be used to trigger the Alarm. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

Actions

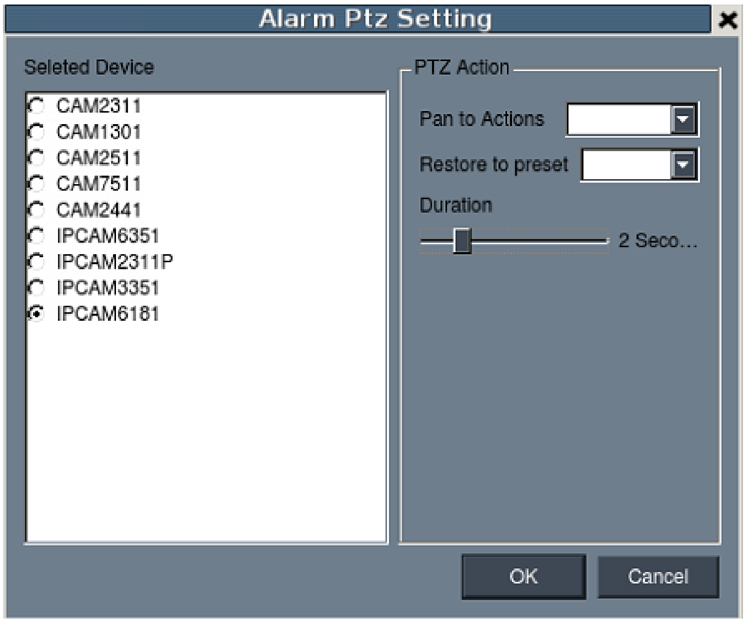
The following alarm actions can be taken when the alarm is triggered:

Event Log

The system issues event messages when the alarm is triggered.

PTZ Control

When the alarm is triggered, a Pan-Tilt-Zoom action can be set to slew the camera to a particular position. For example, clicking on the **Action** button brings up the *PTZ Action Settings* menu. In this menu:



1. Choose a camera from the list.
2. Select a preset point from the **Pan to Preset** dropdown that the camera will pan to.
3. Select the preset that the camera will return to from the **Restore Presets** dropdown.
4. Specify a duration that the camera will stay at the **Pan to Action** preset before returning to the **Restore to Preset** using the **Duration** slider. Click **Apply** to save the settings.
5. Click **OK** to exit the menu.

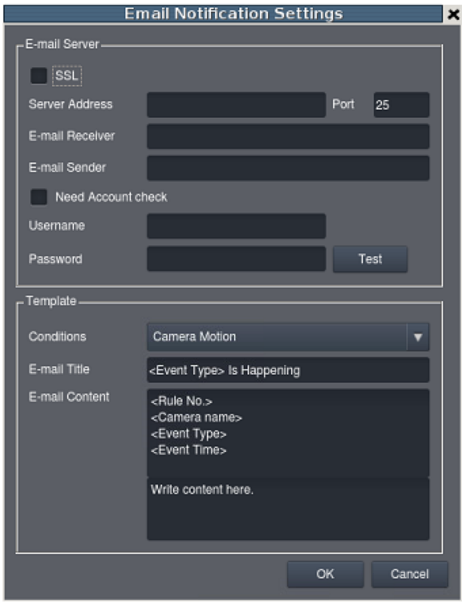
Recording Controls

When the alarm is triggered, the system records video onto the storage. Clicking on the **Action** button will pull up the *Recording Settings* menu.

Use the checkboxes within to select cameras that will be recorded. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

E-Mail

When the alarm is triggered, an E-Mail will be sent. Checking this option will bring up the *E-mail Settings* menu.



Email Notification Settings

E-mail Server

□ SSL

Server Address: Port: 25

E-mail Receiver:

E-mail Sender:

□ Need Account check

Username:

Password:

Template

Conditions: Camera Motion

E-mail Title: <Event Type> Is Happening

E-mail Content:
<Rule No.>
<Camera name>
<Event Type>
<Event Time>

Write content here.

SSL: Tick this option to enable SSL (Secure Sockets Layer) and to enhance security.

Server Address: You may either enter the URL (such as smtp.abc.com) or IP address of the SMTP server that the Server will use to deliver E-mail notifications. The SMTP server configured here must support Unicode Transformation Format-8 (UTF-8) encoding.

E-mail Receiver: Enter one or more E-mail addresses in the **Recipients**: field. These address(es) will receive notifications from the Server. Multiple addresses can be entered by separating individual addresses with semi - colons ";".

E-mail Sender: Enter a valid E-mail address in the field. This address will be the default sender listed in E-mails sent from the Server.

Need Account Check: Tick this option to check.

Username: Enter the user name for the Server email account in the **Username** field.

Password: Enter the password for the Server email account in the **Password** field.

(Optional) Click **Test** to send a test message to the E-mail addresses listed.

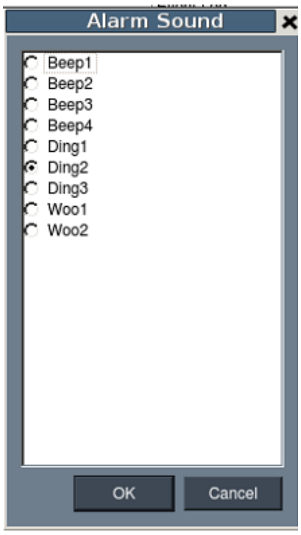
Conditions: Select a condition from the dropdown list to send out an email notification.

E- Mail Title: Enter the subject of your notification E-mails, e.g., Server-xxxsite1notification in the field.

E- Mail Content: Enter a short message in the large field to describe the Server or a surveillance network.

Alarm Sound

When the alarm is triggered, the system will play an audible alarm sound. Clicking on the **Action** button will pull up the *Warning Sound* menu, listing available sounds.



○ Beep1
○ Beep2
○ Beep3
○ Beep4
○ Ding1
● Ding2
○ Ding3
○ Woo1
○ Woo2

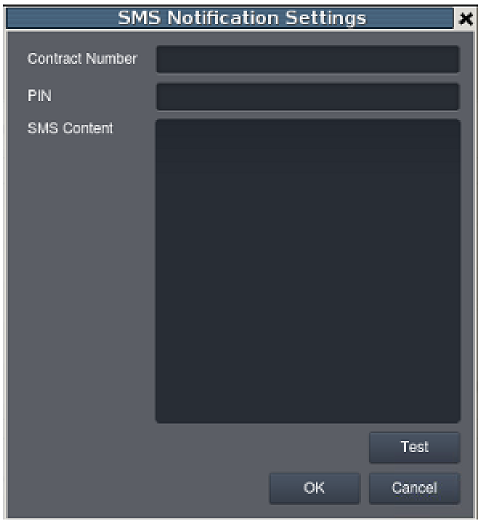
Video Popup / E-Map

When the alarm is triggered, a popup video appears on the local client.

Clicking the **Action** button will pull up a menu.

SMS

When the alarm is triggered, an SMS message will be sent. Checking this option will bring up the *SMS Settings* menu.



Note: Drivers for supported GSM/GPRS modems have already been installed on the server. Currently, only the **WaveCOM-M1206B** is supported. Use COM1 on the Server to connect to a GSM modem.

1. In the **Contact Number** field, enter the phone numbers that will receive SMS notifications. Be sure to include the area code, e.g., “86”, in front of phone numbers. Use commas, “,” to separate individual phone numbers.

2. Use the slider bar to select a delay between the occurrence of an event and SMS message delivery.

3. **(Optional)** If a SIM PIN is required, enter the PIN code in the **PIN** field. Note that applying incorrect PIN code may disable your SIM card.

> **Note:** To change the PIN code, remove the SIM card from your GSM modem. Use a cell phone to change the PIN code and then re -install SIM card into the GSM modem. Changing PIN codes is not recommended because a configuration failure may disable your SIM card.

4. In the **SMS Content** field, type a simple description to include in the outgoing SMS messages

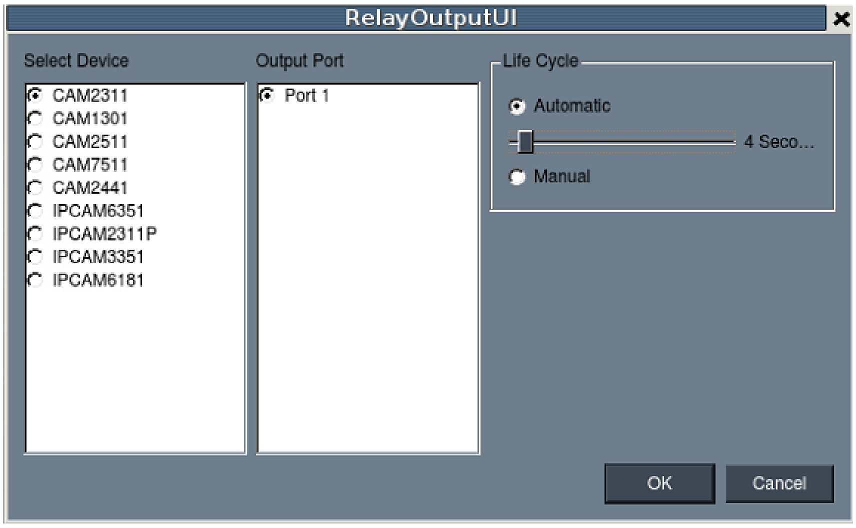
5. **(Optional)** Click **Test** to send a test message to the phone numbers listed.

6. Click the **Apply** button to apply the changes.

7. Click the **OK** button to exit SMS settings.

Relay Output

When the alarm is triggered, a signal will be relayed to an external source such as a light switch, siren, or other external link. Clicking on the **Action** button brings up the *External Relay Settings* menu. In this menu:



Select Device

● CAM2311
○ CAM1301
○ CAM2511
○ CAM7511
○ CAM2441
○ IPCAM6351
○ IPCAM2311P
○ IPCAM3351
○ IPCAM6181

Output Port

● Port 1

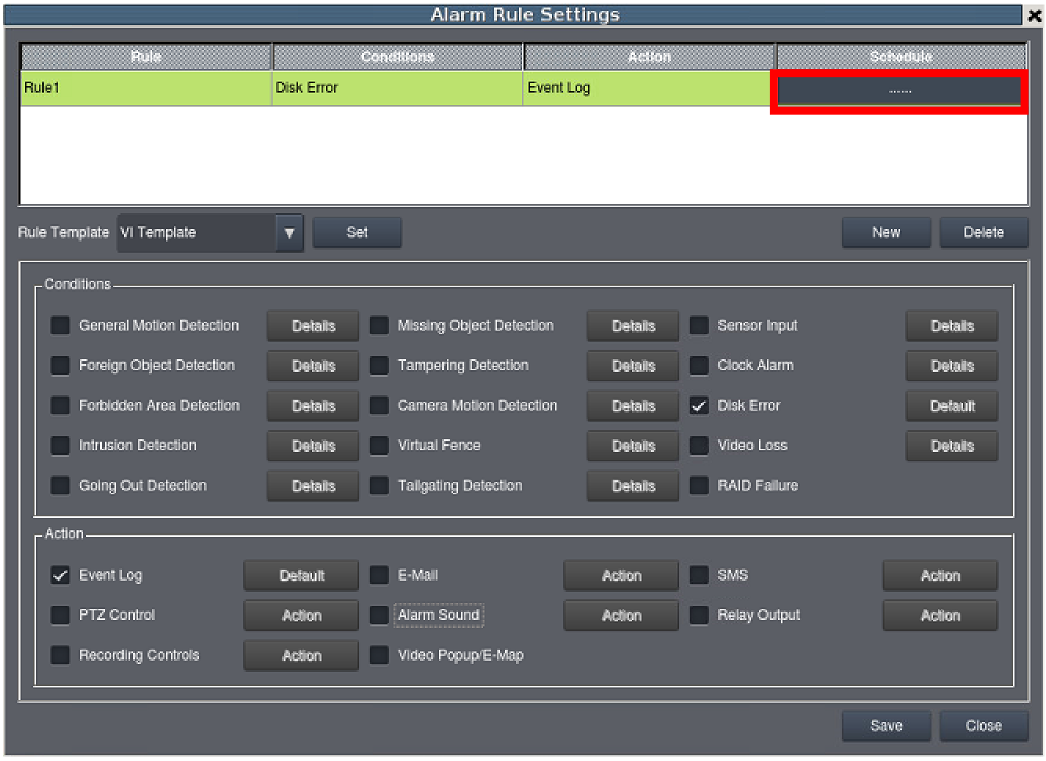
Life Cycle

● Automatic
4 Seco...
○ Manual

1. Choose a camera from the list.
2. Select an output port to relay to.
3. Select output duration, from 0 to 60 seconds.
4. Click the **OK** button to exit the menu.

Alarm Scheduling

When the alarm is created, click the ……button located in the scheduling column of the alarm listing to bring up the *Alarm Rule Schedule* menu. This displays a table with the days of the week as the columns, and hours as the rows, allowing the user to schedule the alarm on exact hours.



Rule	Conditions	Action	Schedule
Rule1	Disk Error	Event Log	......

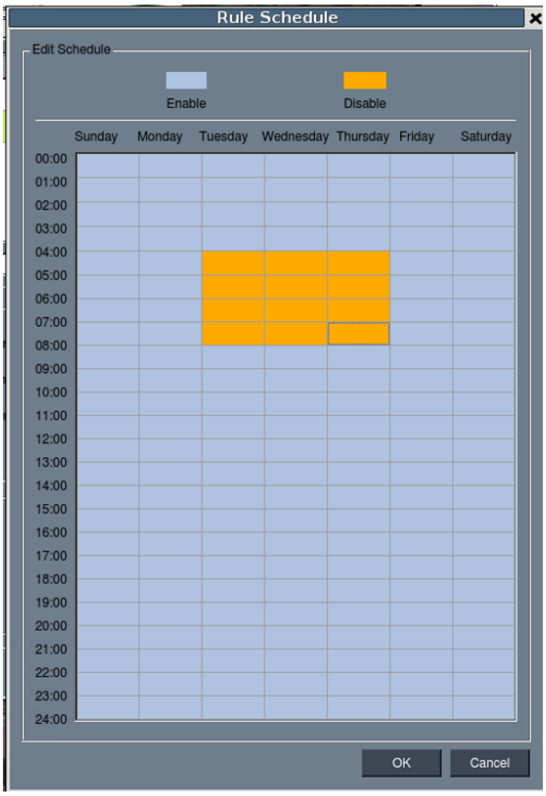
Rule Template: VI Template

Conditions

☐ General Motion Detection	☐ Missing Object Detection	☐ Sensor Input
☐ Foreign Object Detection	☐ Tampering Detection	☐ Clock Alarm
☐ Forbidden Area Detection	☐ Camera Motion Detection	☑ Disk Error
☐ Intrusion Detection	☐ Virtual Fence	☐ Video Loss
☐ Going Out Detection	☐ Tailgating Detection	☐ RAID Failure

Action

☑ Event Log	☐ E-Mail	☐ SMS
☐ PTZ Control	☐ Alarm Sound	☐ Relay Output
☐ Recording Controls	☐ Video Popup/E-Map	



From this menu, use the following steps to schedule the alarm:

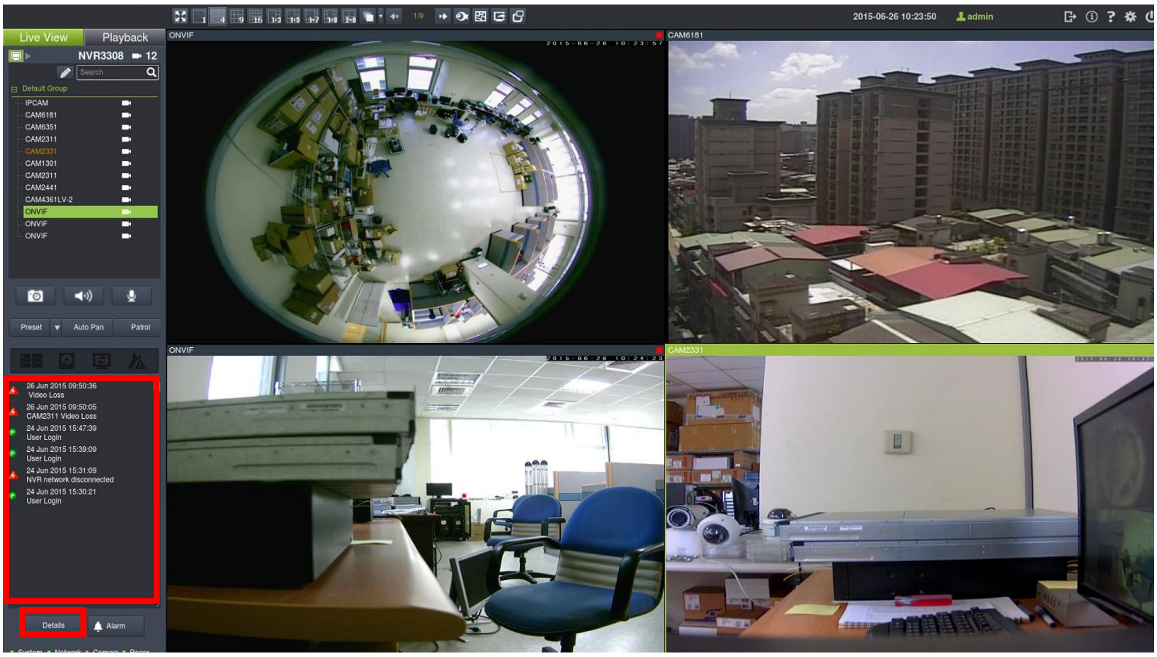
1. Choose the rule that you wish to apply the schedule to.
2. Click the **Enable** or **Disable** button to bring up a “paintbrush.”
3. Click the cursor on the table to “paint” in a schedule. You may click and drag to paint a wide area.

For example, if you wish to disable the alarm on Tuesday at 6pm, you would click the box Tuesday-18:00. Disabled time periods are highlighted in yellow.

Click the **OK** button to apply the changes and exit the menu.

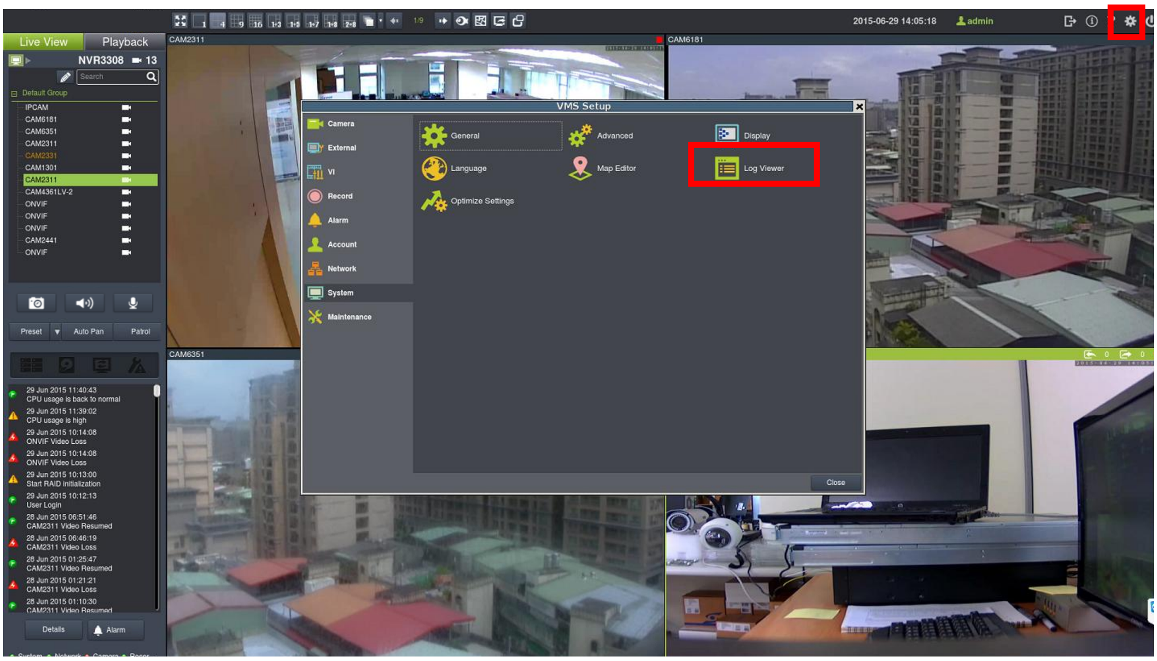
9.2. Event Log

The event log is a comprehensive repository of all the events that occur on the system. You can find the event log on the left corner of the live view page. Click on the **Details** button to see the View Log window.



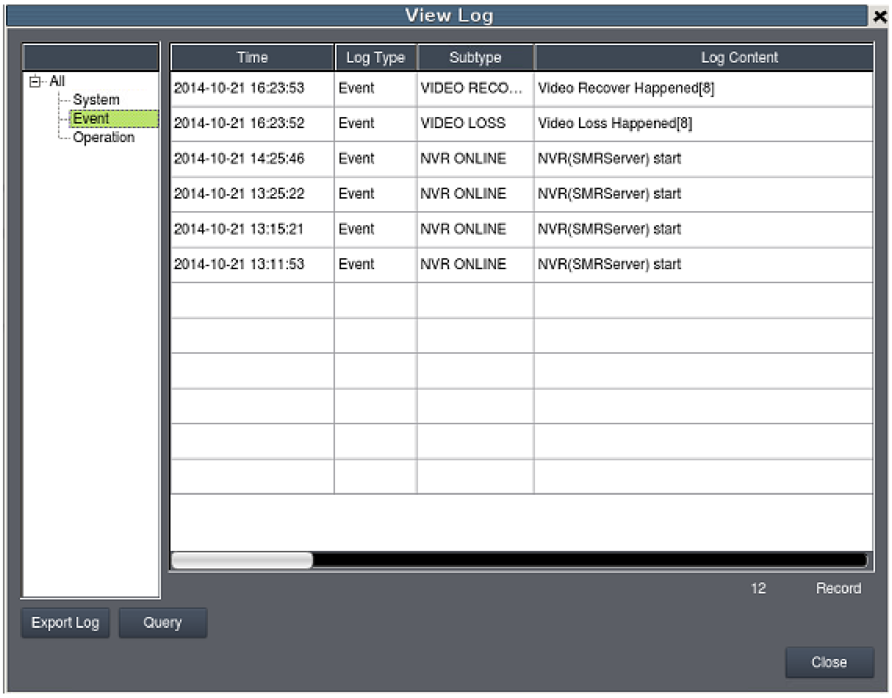
```
26 Jun 2015 09:50:36
 Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected
24 Jun 2015 15:30:21
User Login
```

Or click ⚙ to bring out **VMS Setup** window and select **System** > **Log Viewer**. The *Log Viewer* window will display.



```
29 Jun 2015 11:40:43
CPU usage is back to normal
29 Jun 2015 11:39:02
CPU usage is high
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
```

The view log splits into three types, System, concerning with individual modules, Event, concerning with cameras and Operation, concerning with users.



Time	Log Type	Subtype	Log Content
2014-10-21 16:23:53	Event	VIDEO RECO…	Video Recover Happened[8]
2014-10-21 16:23:52	Event	VIDEO LOSS	Video Loss Happened[8]
2014-10-21 14:25:46	Event	NVR ONLINE	NVR(SMRServer) start
2014-10-21 13:25:22	Event	NVR ONLINE	NVR(SMRServer) start
2014-10-21 13:15:21	Event	NVR ONLINE	NVR(SMRServer) start
2014-10-21 13:11:53	Event	NVR ONLINE	NVR(SMRServer) start

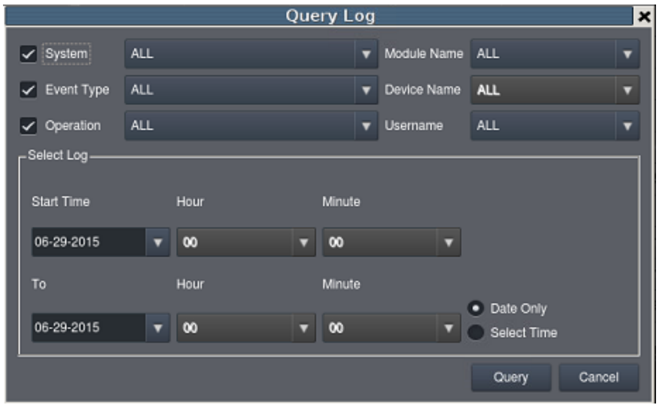
12 Record

9.2.1. Exporting a Log

If log entries exist, they may be exported by clicking on the **Export Log** button at the bottom of the View *Log* screen. This will open a dialog box, which prompts users to choose a location, and fill in a name for the saved log. Fill out the location and filename information and click **OK** to save the log file.

9.2.2. Searching the Event Log

Within the *View Log* screen, click the **Query** button to bring out the *Query Log* dialog box.



☑ System ALL Module Name ALL
☑ Event Type ALL Device Name ALL
☑ Operation ALL Username ALL

Select Log

Start Time 06-29-2015 Hour 00 Minute 00

To 06-29-2015 Hour 00 Minute 00

● Date Only
○ Select Time

Within this dialog, users may choose to narrow the search to the three major event types by selecting the checkbox beside the event type:

System

These are errors that occur within individual system modules. In the corresponding selection box, the user can specify a severity (debug, warning, error and fatal in increasing severity) of the event. The user may also choose to search all of the severities.

Event Type

These include errors that occur with cameras. Events include motion detection, video loss, sensor input, clock alarm, disk error and RAID failure. The user may also choose to search over all these types.

Operation

These events include the console startup and stop, system usage, and other events that occur during system operation.

Module Name

The corresponding subfield for *System Type* is *Module Name*. In this selection box, the user can specify a module to search for errors on. The user may also choose to search over all modules by choosing **All**.

Device Name

This subfield contains a list of all the cameras installed on the system. The events can be further narrowed to focus on a single camera by choosing it, or the search can be done over all cameras by choosing **All**.

User Name

Using the *User Name* subfield a search can be narrowed down to an individual user. This selection list contains all the users configured on the system. All the users can be included by selecting **All.**

Performing a Search

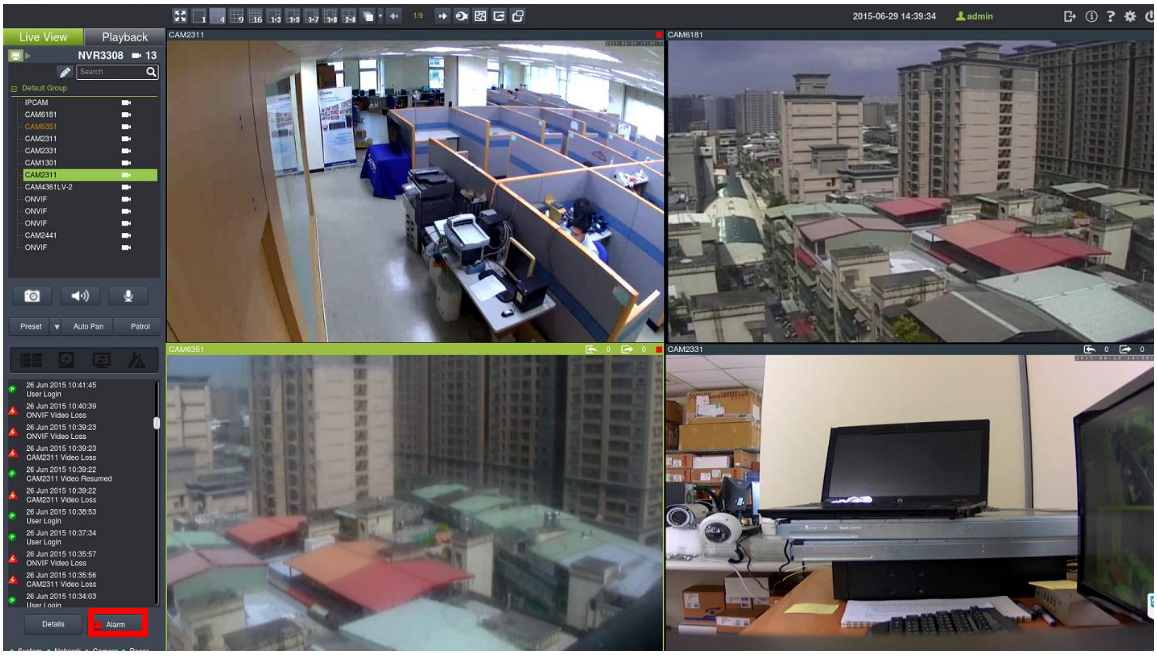
To perform a search of the log files:

1. If desired, narrow the search by selecting an event type and subfield to search over. More than one event type can be searched.
2. Choose a start date and an end date to search over using the calendar drop-downs.
3. If desired, click **Select time** and select an hour and minute for the start and end times to further narrow the search.
4. Click the **Query** button. The results will show in the main *View Log Screen*.

9.2.3. System Alarm View

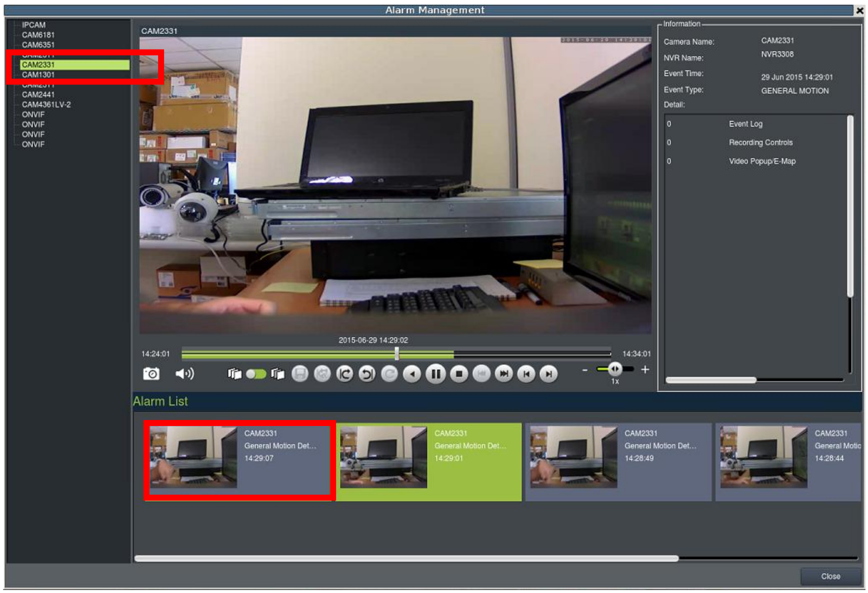
When there an alarm occurred, the alarm icon will flash. Click on the flashing Alarm button on the left corner of the Live View page to see and manage the alarms.

NOTE: The VI detection should be set beforehand and the Video Popup/E-Map should be enabled to activate this functionality. Go to VMS Setup > Alarm > Rule > Action > Video Popup/E-map to activate this functionality.



26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login

The following window will appear. Click on the flashing camera model to see the detailed information. And click on the video footage and use the icons to play the video.



Information

Camera Name: CAM2331
NVR Name: NVR3308
Event Time: 29 Jun 2015 14:29:01
Event Type: GENERAL MOTION
Detail:

0 Event Log
0 Recording Controls
0 Video Popup/E-Map

CAM2331
General Motion Det...
14:29:07

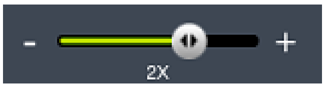
CAM2331
General Motion Det...
14:29:01

CAM2331
General Motion Det...
14:28:49

CAM2331
General Motic
14:28:44

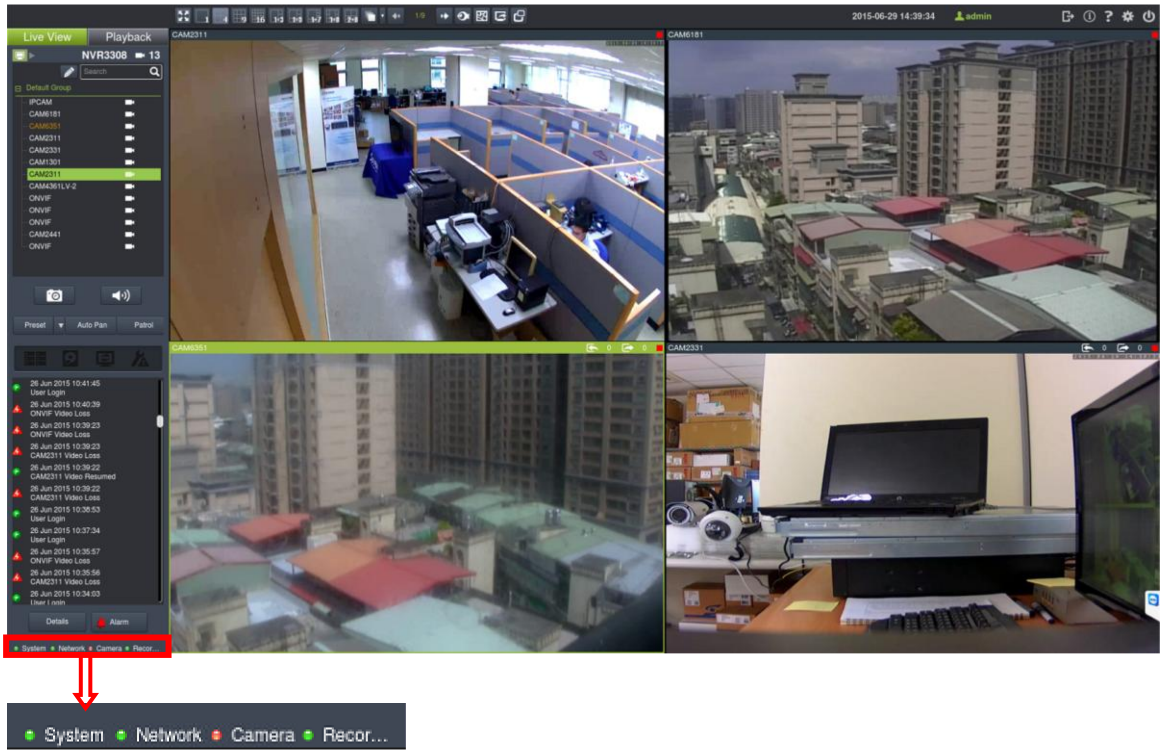
The following table explains the buttons:

📷	Snapshot
🔊	Audio volume
- ● + 60 Min	Time range can be set when viewing the playback.
⧉ ○● ⧉	Full frame mode
⧉ ●○ ⧉	Key frame mode
💾	Saves video clips/Exports selected clips
⊗	Clear all the Cue-Ins and Cue-Outs
|↻	Set Cue-In marker for clip start
↺|	Set Cue-In marker for clip end
↻	Automatic reply the clip. (From Cue-in to Cue-Out)
◀	Play backwards
▶	Starts video playback
⏸	Pause video playback
■	Stops video playback.
|◀	Jumps to the previous frame
▶|	Jumps to the next frame
⏮	Jumps to the previous segment

⏭	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

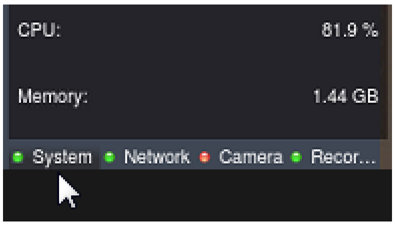
9.2.4. Overall Status

See the overall status on the left corner of the Live View page. Red light indicates something is not right while the green light shows everything is ok.



System Status

Hover over the System Status Icon to see the CPU and Memory usage.

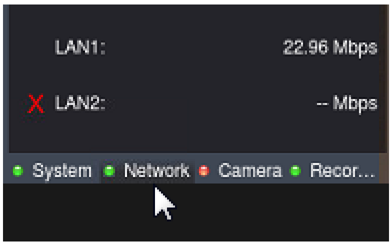


CPU: 81.9 %

Memory: 1.44 GB

Network Status

Hover over the Network Status Icon to see the network status.

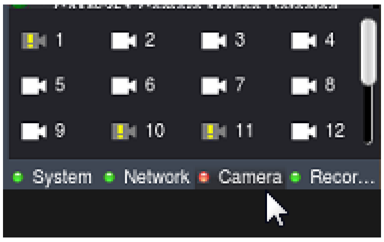


LAN1: 22.96 Mbps

X LAN2: -- Mbps

Camera Status

Hover over the Camera Status Icon to see the camera status and see which one is out of order.



Recording Status

The overall recording status is shows as green or red.

Chapter 10 Search and Playback

In many cases, such as investigations or for reference purposes, it may be useful to be able to replay video streams. The Server has the ability to store video from the IP cameras, as well as playback and export this video information.

10.1. Introduction

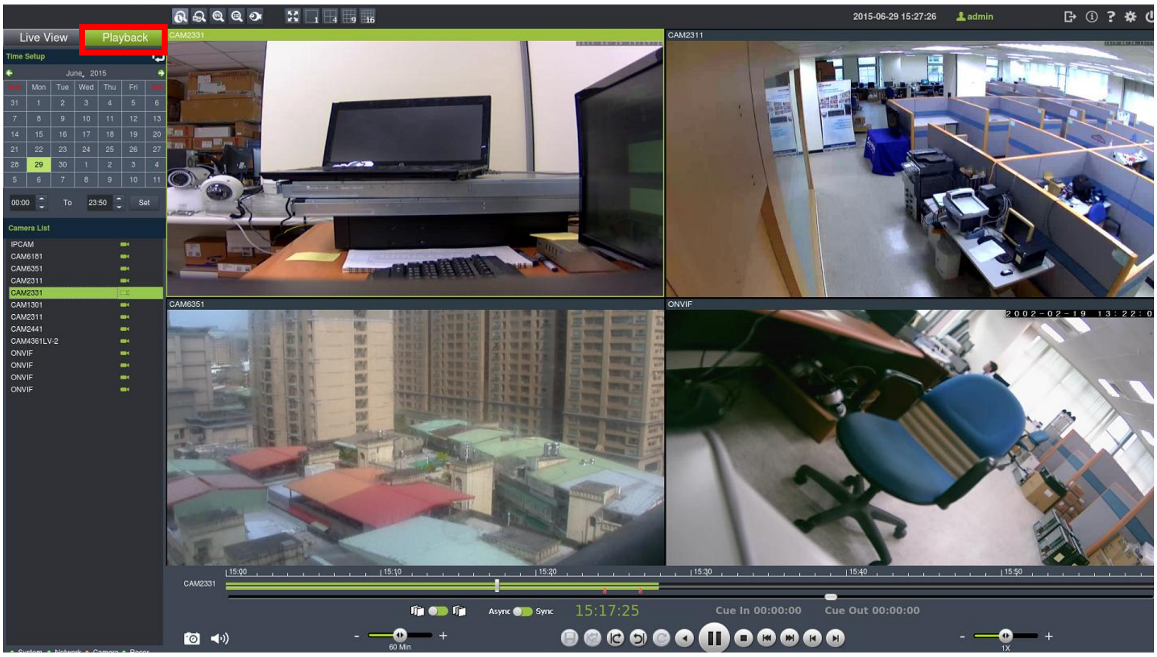
Note: You must be logged **into** a server to access playback functionality.

Click on the *Playback* tab in the live view screen.

The VMS has 3 distinct playback functions:

- Time Search – Plays back according to a time period specified by the user.
- VI Search – Applies VI functionalities to a recorded video stream.
- Event Search – Searches the video stream for distinct events.

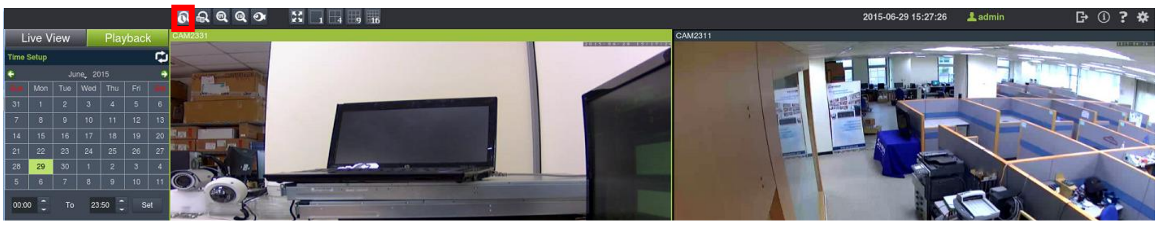
Note: Event Search is recommended rather than VI Search, since VI Search uses more bandwidth.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

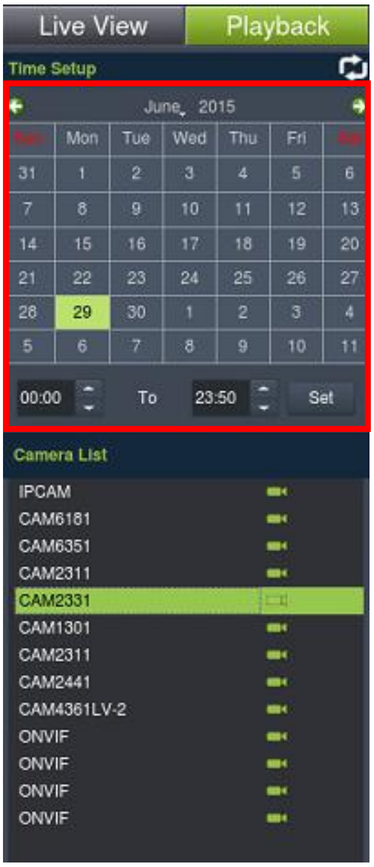
10.2. Time Search

10.2.1. Creating a Time Search



Specified Time

Use the arrows, calendar and time boxes to specify a specific period for search/playback.



June, 2015

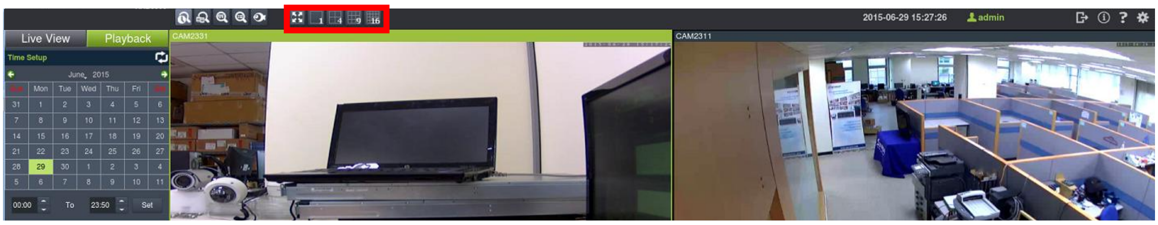
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

00:00 To 23:50 Set

IPCAM
CAM6181
CAM6351
CAM2311
CAM2331
CAM1301
CAM2311
CAM2441
CAM4361LV-2
ONVIF
ONVIF
ONVIF
ONVIF

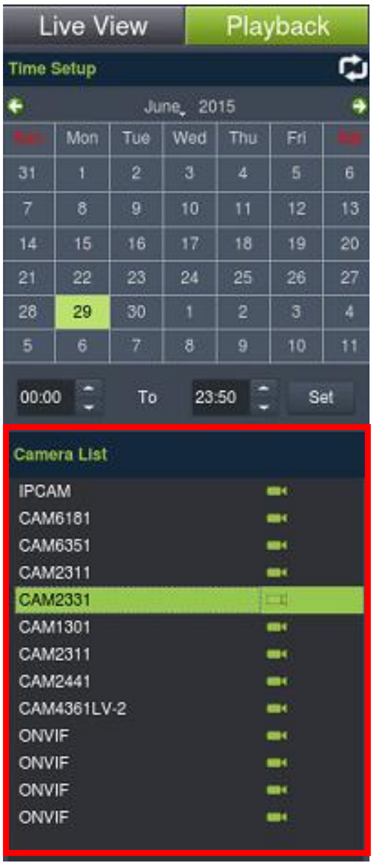
10.2.2. Use of Various Views Selection

Users have the option of viewing the fisheye view or up to 16 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.



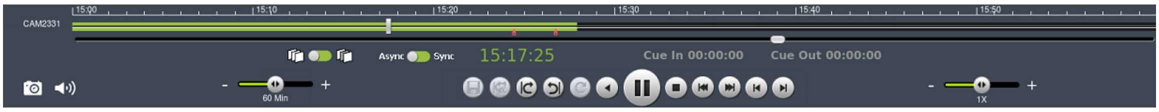
10.2.3. Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



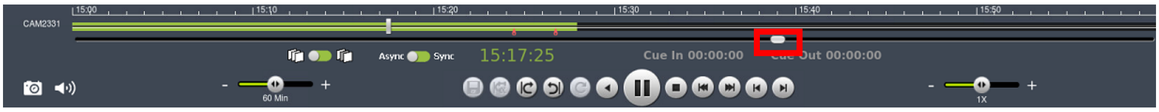
10.2.4. Timeline

After choosing the cameras to view, the timeline for the camera is displayed below the video window.



The timeline window displays a graphic representation of the video information available for the camera on the date and timeframe you have chosen in the *Select Date* window.

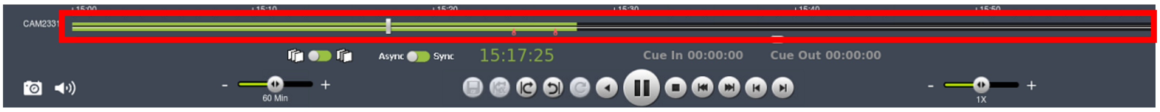
The timeline will, at most, show a period of a little more than 3 hours. If the timeframe that you desire to view is larger than this, the remaining portion of the timeline can be viewed by using the **scrollbar** located beneath the timeline.



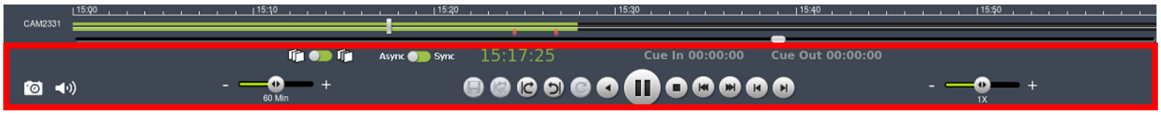
The amount of time displayed in the timeline can also be adjusted using the **slider** located next to the scrollbar. Sliding the indicator toward the right will cause a smaller amount of time to be displayed along the length of the timeline.

10.2.5. Playback

Once a timeline has been loaded, you may choose the point to begin playback. This is done by clicking the **timeline**. After selecting the start point you may start playback.



To start playback of a camera's video feed, ensure that the video is selected. Select feeds by clicking the corresponding pane, timeline, or camera name. Once you have selected a camera, you may use the buttons to control the playback. Playback time is denoted above the control buttons.



Note: The system may take a while to buffer the video before playback starts. A status line above the timeline will indicate portions that have been buffered. Jumping to unbuffered points in the video will cause the system to display an error message.

Clicking on a selected portion of the timeline will cause playback to jump to the point that you have clicked on. You must start playback separately for each feed you wish to view.

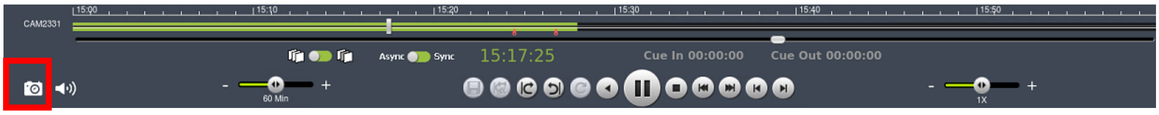
The following table explains the buttons:

Sync ○ Async	Sync all the views to play videos from the same period of time. While in the Sync mode, the view cannot be changed. Async, undo syn, different views can be selected.
📷	Snapshot
🔊	Audio volume
- ● + 60 Min	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
💾	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start
	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
◀	Play backwards

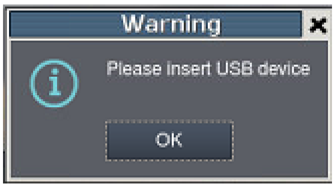
▶	Starts video playback
⏸	Pause video playback
⏹	Stops video playback.
⏮	Jumps to the previous frame
⏭	Jumps to the next frame
⏮	Jumps to the previous segment
⏭	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

Capturing Screenshot

1. Click the **Snapshot** button located in the button area.



The snapshot will be stored in the USB device. Please have your USB device ready.



Warning

Please insert USB device

OK

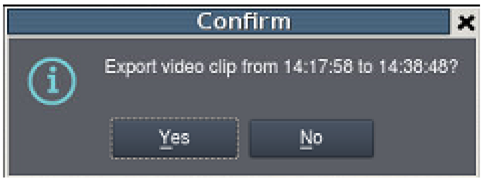
Capturing Video Clip

1. Make sure that the video clip is playing.

2. When the beginning of the segment to be captured is reached, click the **Cue In** button.

3. When the end of the segment to be captured is reached, click the **Cue Out** button.

4. A popup window will appear for confirmation.



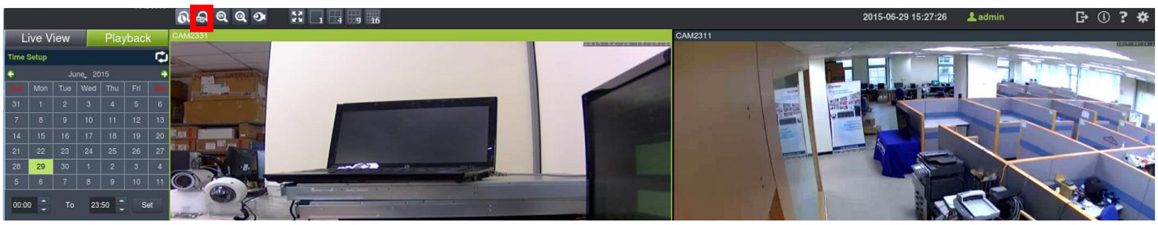
Export video clip from 14:17:58 to 14:38:48?

5. Click **Yes** when confirmed. Click **No** and redefine the Cue-In and Cue-Out.

6. The video will be stored in the USB device. Please have your USB device ready.

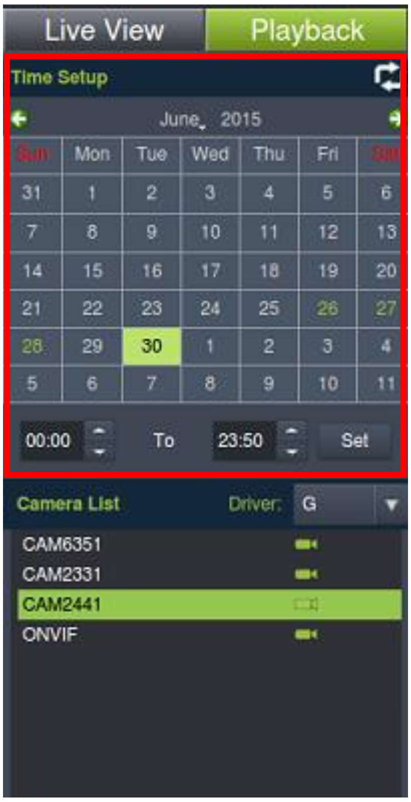
10.3. Backup Search

10.3.1. Creating a Backup Search



Specified Time

Use the arrows, calendar and time boxes to specify a specific period for search/playback.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

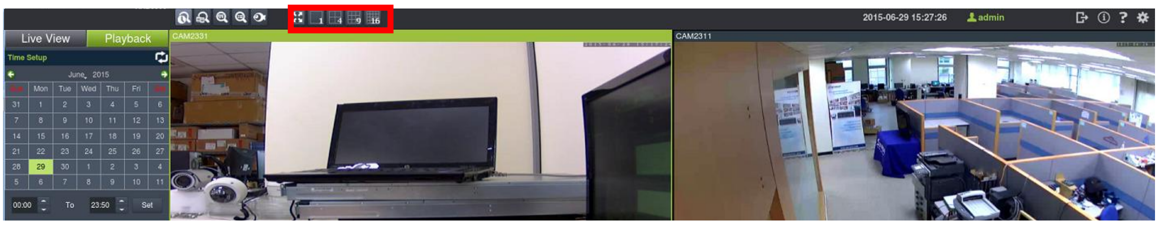
00:00 To 23:50 Set

Camera List Driver: G

CAM6351
CAM2331
CAM2441
ONVIF

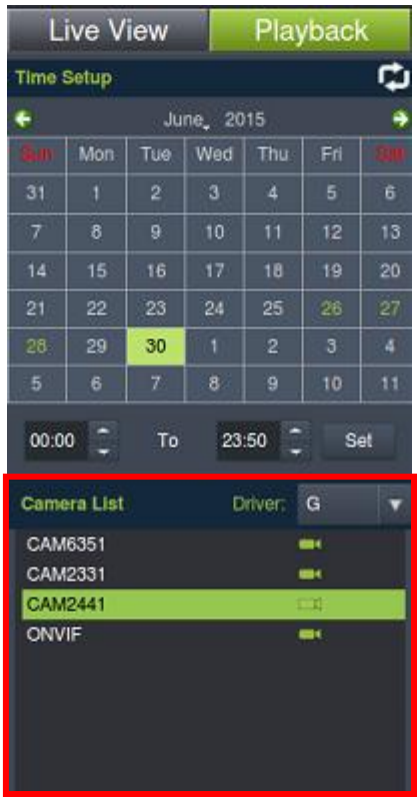
10.3.2. Use of Various Views Selection

Users have the option of viewing the fisheye view or up to 16 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.



10.3.3. Camera Selection

Once a time period has been selected, you can select the source driver and the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

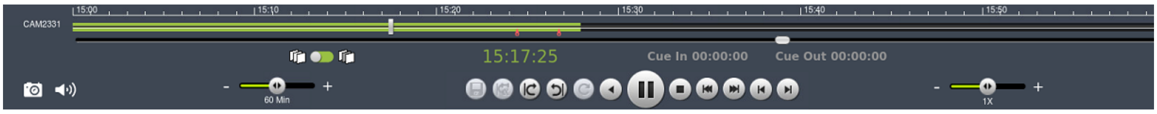
00:00 To 23:50 Set

Camera List Driver: G

CAM6351
CAM2331
CAM2441
ONVIF

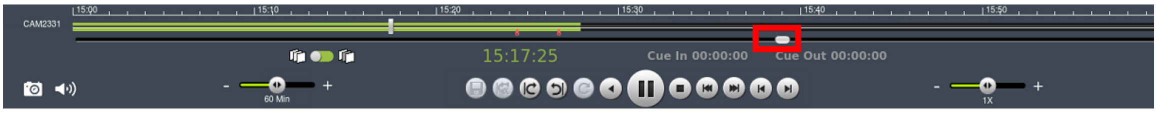
10.3.4. Timeline

After choosing the cameras to view, the timeline for the camera is displayed below the video window.



The timeline window displays a graphic representation of the video information available for the camera on the date and timeframe you have chosen in the *Select Date* window.

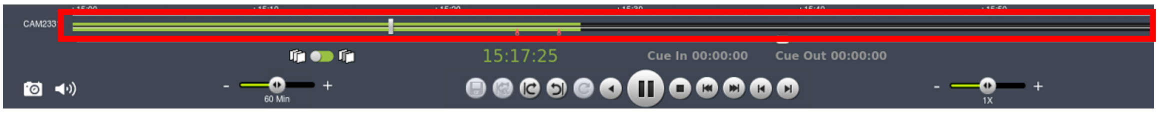
The timeline will, at most, show a period of a little more than 3 hours. If the timeframe that you desire to view is larger than this, the remaining portion of the timeline can be viewed by using the **scrollbar** located beneath the timeline.



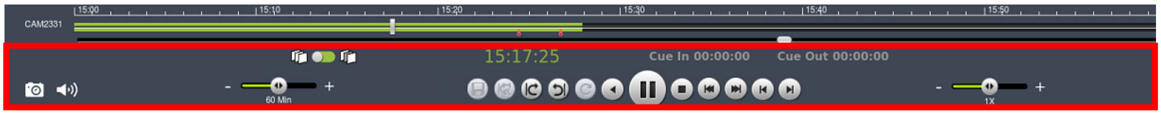
The amount of time displayed in the timeline can also be adjusted using the **slider** located next to the scrollbar. Sliding the indicator toward the right will cause a smaller amount of time to be displayed along the length of the timeline.

10.3.5. Playback

Once a timeline has been loaded, you may choose the point to begin playback. This is done by clicking the **timeline**. After selecting the start point you may start playback.



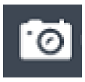
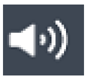
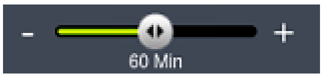
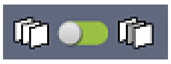
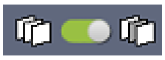
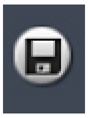
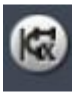
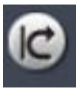
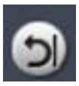
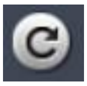
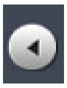
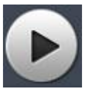
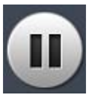
To start playback of a camera's video feed, ensure that the video is selected. Select feeds by clicking the corresponding pane, timeline, or camera name. Once you have selected a camera, you may use the buttons to control the playback. Playback time is denoted above the control buttons.



Note: The system may take a while to buffer the video before playback starts. A status line above the timeline will indicate portions that have been buffered. Jumping to unbuffered points in the video will cause the system to display an error message.

Clicking on a selected portion of the timeline will cause playback to jump to the point that you have clicked on. You must start playback separately for each feed you wish to view.

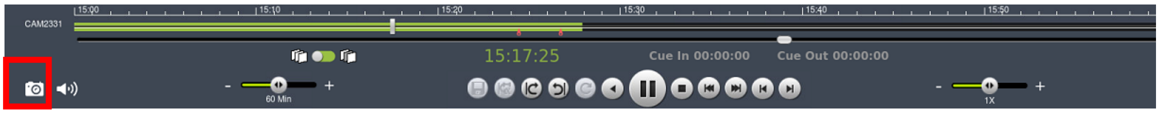
The following table explains the buttons:

	Snapshot
	Audio volume
	Time range can be set when viewing the playback.
	Full frame mode
	Key frame mode
	Saves video clips/Exports selected clips
	Clear all the Cue-Ins and Cue-Outs
	Set Cue-In marker for clip start
	Set Cue-In marker for clip end
	Automatic reply the clip. (From Cue-in to Cue-Out)
	Play backwards
	Starts video playback
	Pause video playback

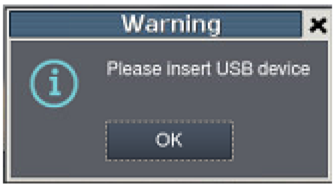
■	Stops video playback.
⏮	Jumps to the previous frame
⏭	Jumps to the next frame
⏪	Jumps to the previous segment
⏩	Jumps to the next segment
- ● + 2X	The play speed can be adjusted from 1x to 8x.

Capturing Screenshot

1. Click the **Snapshot** button located in the button area.



The snapshot will be stored in the USB device. Please have your USB device ready.



Please insert USB device

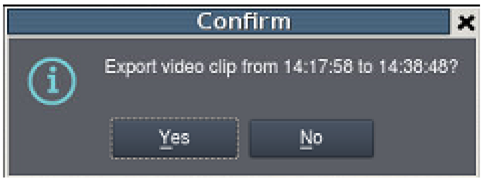
Capturing Video Clip

1. Make sure that the video clip is playing.

2. When the beginning of the segment to be captured is reached, click the **Cue In** button.

3. When the end of the segment to be captured is reached, click the **Cue Out** button.

4. A popup window will appear for confirmation.



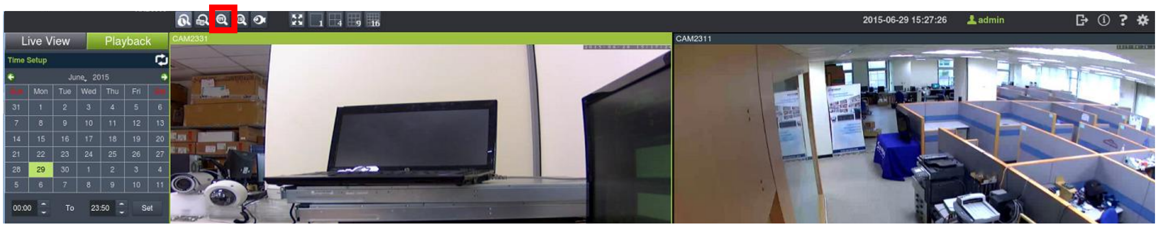
Export video clip from 14:17:58 to 14:38:48?

5. Click **Yes** when confirmed. Click **No** and redefine the Cue-In and Cue-Out.

6. The video will be stored in the USB device. Please have your USB device ready.

10.4. VI Search

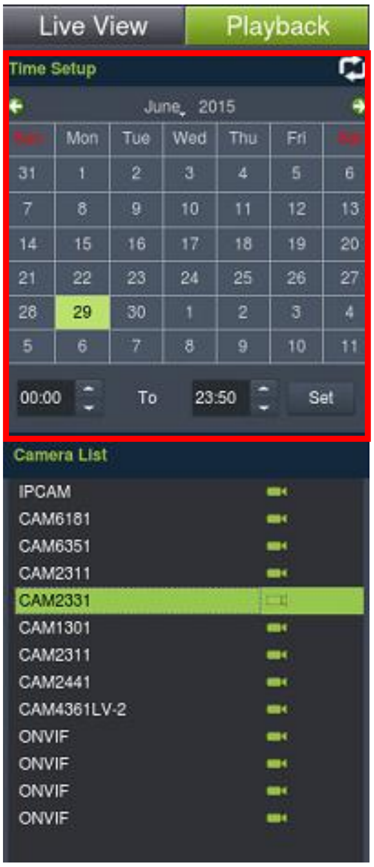
A VI search involves applying VI to existing recorded video in order to locate a specific event or action. To access the VI search, click the *VI icon* next to the fisheye icon in the button area.



10.4.1. Creating a VI Search

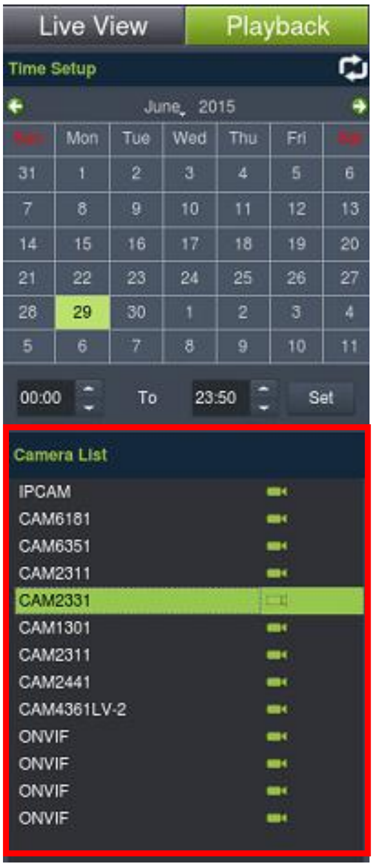
Time Selection

Use the arrows, calendar and time boxes to specify a specific period for search/playback. Once a date is selected, clicking on the boxes will allow you to specify a specific period to search/playback in 10 minute increments.



Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

00:00 To 23:50 Set

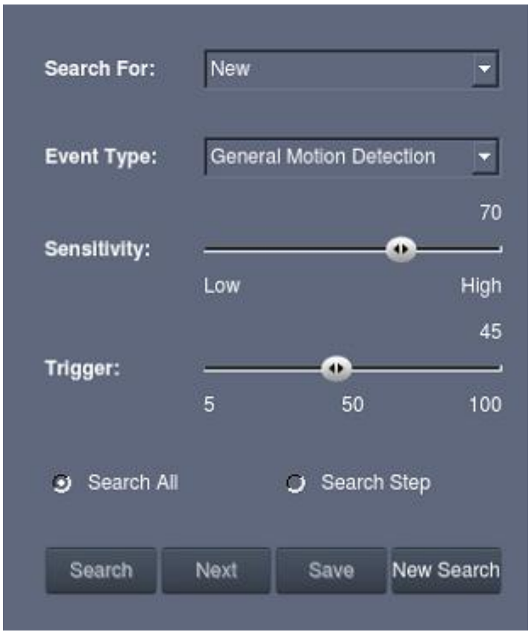
Camera List

IPCAM
CAM6181
CAM6351
CAM2311
CAM2331
CAM1301
CAM2311
CAM2441
CAM4361LV-2
ONVIF
ONVIF
ONVIF
ONVIF

Select a camera to perform the VI search on by clicking its entry. This will display an initial thumbnail of the camera output.

Setting New Search Criteria

To create a New VI search, follow directions in the following sections to set up the VI search.



Search For: New

Event Type: General Motion Detection

Sensitivity: 70

Trigger: 45

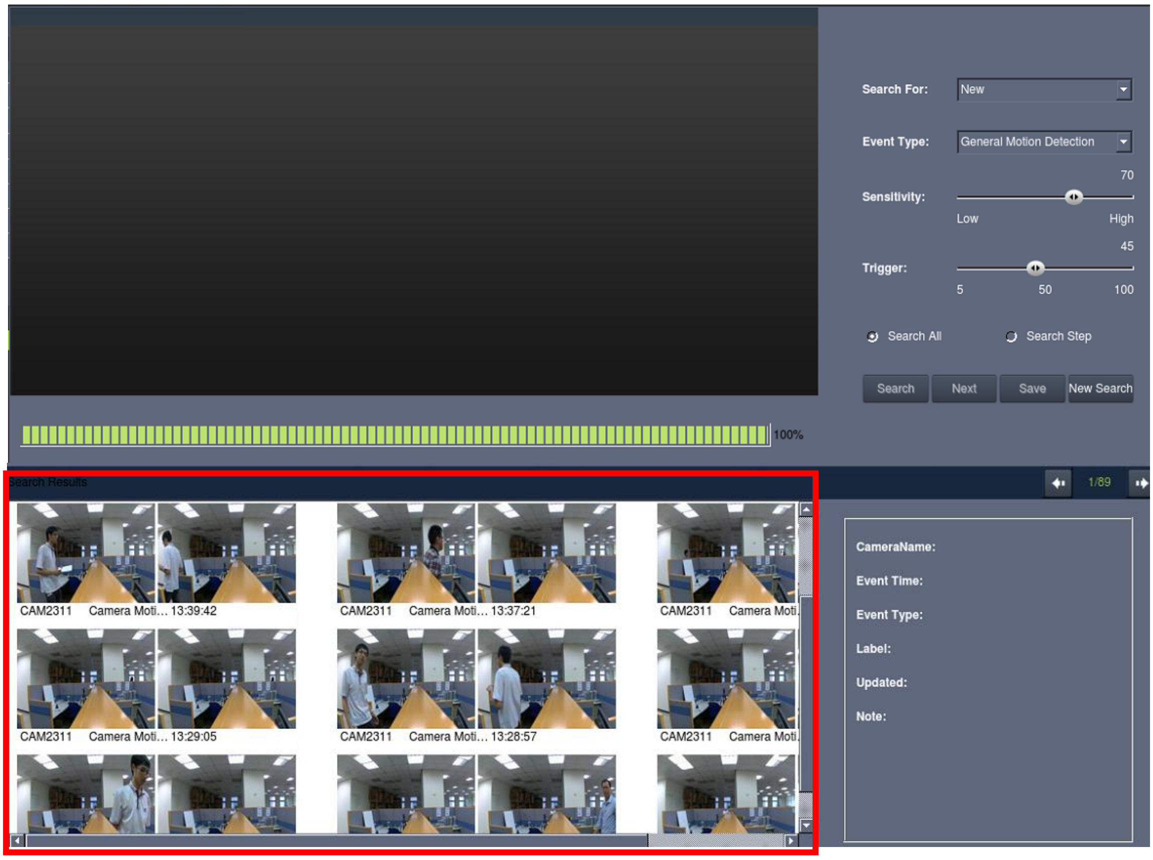
● Search All ○ Search Step

1. **New** in the playback control.
2. Select an **Event Type.**
3. Define the **Sensitivity and the Trigger.**
4. **Search Type**
   - **Search All -** Finds all events within the search range that trigger the VI set up.
   - **Search Step** – Finds the first event that triggers the VI, then stops. The next event can be found by repeating the same search.
5. Click **Search** to begin the VI Search.
6. Click Save to save the VI search. The system will prompt you for a name. Saved VI searches can also be retrieved using the **Search for** dropdown or by clicking the **Next** button.
7. Click **New Search**, when there are more searches to do.

10.4.2. Using the Search Results

Selecting the Result

Search result thumbnail(s) will be displayed in the results box.



Search For: New

Event Type: General Motion Detection

Sensitivity: 70

Trigger: 45

Clicking the thumbnail will select the detection instance. The following information fields are available for each instance:

- **Camera Name** – The camera used to capture the video.
- **Event Time** – The time the event occurred.
- **Event Type** – The type of VI detection that the event triggered.
- **Label** – A user-defined label (optional).
- **Updated -** The last time the event was updated.

Result Playback

Once a result is selected by clicking on it, playback can be started by double clicking on the thumbnail. Alternatively, you may right-click the thumbnail and click **Play**. A ten minute clip containing the event will begin playing, with the start time synchronized with the start of the event.

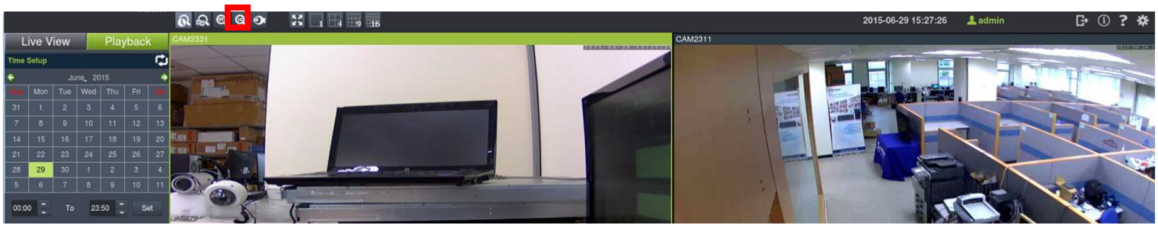
The following functions are available for playback:

📷	Snapshot
🔊	Audio volume
- ◉ + 60 Min	Time range can be set when viewing the playback.
⧉ ○ ⧉	Full frame mode
⧉ ● ⧉	Key frame mode
💾	Saves video clips/Exports selected clips
⏮	Clear all the Cue-Ins and Cue-Outs
↻	Set Cue-In marker for clip start
↺	Set Cue-In marker for clip end
⟳	Automatic reply the clip. (From Cue-in to Cue-Out)
◀	Play backwards
▶	Starts video playback
⏸	Pause video playback
⏹	Stops video playback.
⏮	Jumps to the previous frame
⏭	Jumps to the next frame

⏮	Jumps to the previous segment
⏭	Jumps to the next segment
	The play speed can be adjusted from 1x to 8x.

10.5. Event Search

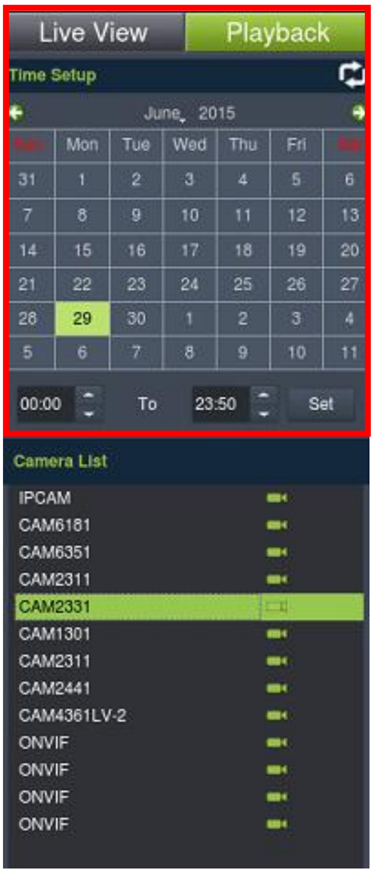
An Event search involves searching for multiple tagged events over one more cameras. To access the Event search, click the *Event Search icon* next to the VI Search icon in the button area.



10.5.1. Creating an Event Search

Time Selection

Use the arrows, calendar and time boxes to specify a specific period for search/playback. Once a date is selected, clicking on the boxes will allow you to specify a specific period to search/playback in 10 minute increments.

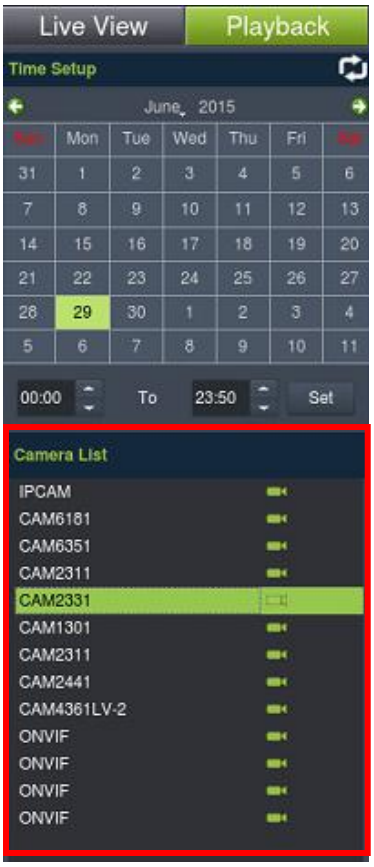


Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

IPCAM
CAM6181
CAM6351
CAM2311
CAM2331
CAM1301
CAM2311
CAM2441
CAM4361LV-2
ONVIF
ONVIF
ONVIF
ONVIF

Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

00:00 To 23:50 Set

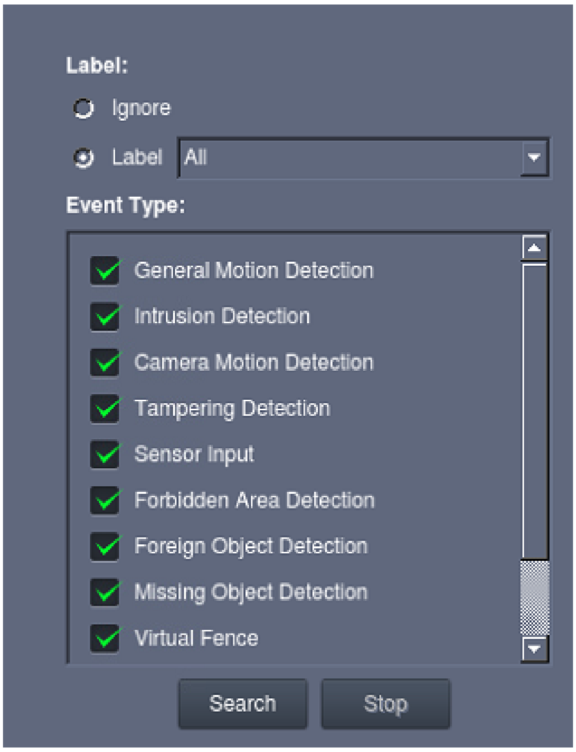
Camera List

IPCAM
CAM6181
CAM6351
CAM2311
CAM2331
CAM1301
CAM2311
CAM2441
CAM4361LV-2
ONVIF
ONVIF
ONVIF
ONVIF

Select a camera to perform the Event search on by clicking its entry. This will display an initial thumbnail of the camera output.

Setting Event Search Criteria

1. Selecting **Ignore** will search for all labels. Choose an **Event Type** and/or a **Label** to search for.



Label:

○ Ignore

● Label All

Event Type:

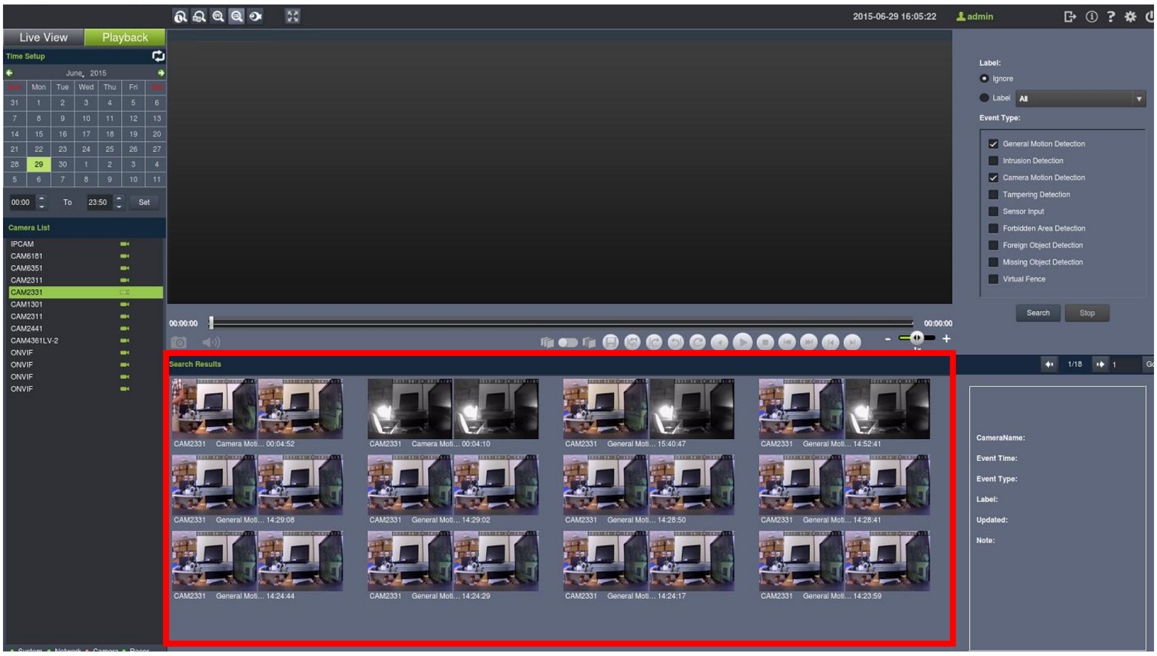
☑ General Motion Detection
☑ Intrusion Detection
☑ Camera Motion Detection
☑ Tampering Detection
☑ Sensor Input
☑ Forbidden Area Detection
☑ Foreign Object Detection
☑ Missing Object Detection
☑ Virtual Fence

2. Click **Search** to begin the search. Results will display in the *Search Results* panel.

10.5.2. Using the Search Results

Selecting the Result

Search result thumbnail(s) will be displayed in the results box.



June 2015

00:00 To 23:50 Set

Camera List: IPCAM, CAM6181, CAM6351, CAM2311, CAM2331, CAM1301, CAM2311, CAM2441, CAM4361LV-2, ONVIF, ONVIF, ONVIF, ONVIF

Label:
● Ignore
○ Label All

Event Type:
☑ General Motion Detection
□ Intrusion Detection
☑ Camera Motion Detection
□ Tampering Detection
□ Sensor Input
□ Forbidden Area Detection
□ Foreign Object Detection
□ Missing Object Detection
□ Virtual Fence

Search Results

CAM2331 Camera Moti... 00:04:52
CAM2331 Camera Moti... 00:04:10
CAM2331 General Moti... 15:40:47
CAM2331 General Moti... 14:52:41
CAM2331 General Moti... 14:29:08
CAM2331 General Moti... 14:29:02
CAM2331 General Moti... 14:28:50
CAM2331 General Moti... 14:28:41
CAM2331 General Moti... 14:24:44
CAM2331 General Moti... 14:24:29
CAM2331 General Moti... 14:24:17
CAM2331 General Moti... 14:23:59

CameraName:
Event Time:
Event Type:
Label:
Updated:
Note:

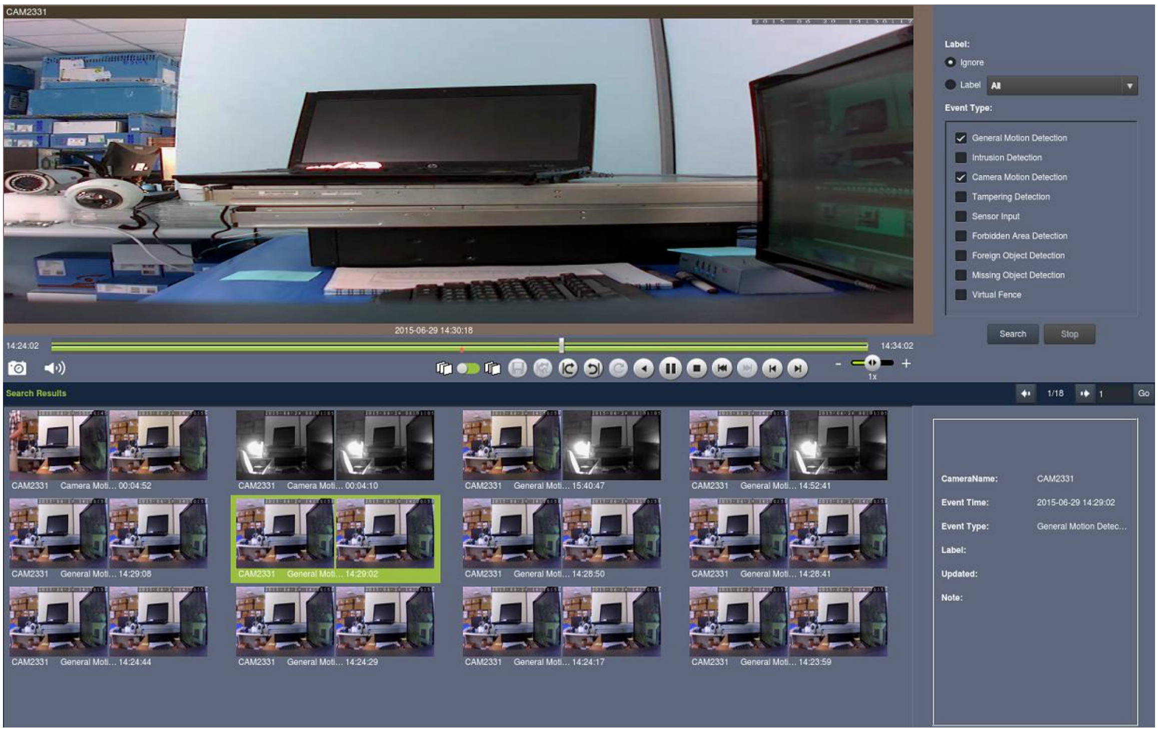
- **Camera Name** – The camera used to capture the video.
- **Event Time** – The time the event occurred.
- **Event Type** – The type of VI detection (if any) that the event triggered (optional).
- **Label** – A user-defined label (optional).
- **Updated -** The last time the event was updated.

Result Playback

Once a result is selected by clicking on it, playback can be started by double clicking on the thumbnail. Alternatively, you may right-click the thumbnail and click **Play**. A ten minute clip containing the event will begin playing, with the start time synchronized with the start of the event.

Synchronize Playback can show you results of different cameras in the same period of time via dragging the cameras you'd like to compare to the view area.

Label can be added as Mark, Check, Clear and Suspicious.



CAM2331
2015-06-29 14:30:18
14:24:02
14:34:02
1x
Search Results
CAM2331 Camera Moti... 00:04:52
CAM2331 Camera Moti... 00:04:10
CAM2331 General Moti... 15:40:47
CAM2331 General Moti... 14:52:41
CAM2331 General Moti... 14:29:08
CAM2331 General Moti... 14:29:02
CAM2331 General Moti... 14:28:50
CAM2331 General Moti... 14:28:41
CAM2331 General Moti... 14:24:44
CAM2331 General Moti... 14:24:29
CAM2331 General Moti... 14:24:17
CAM2331 General Moti... 14:23:59
Search
Stop
1/18
Go

Label:

● Ignore

○ Label All

Event Type:

☑ General Motion Detection
☐ Intrusion Detection
☑ Camera Motion Detection
☐ Tampering Detection
☐ Sensor Input
☐ Forbidden Area Detection
☐ Foreign Object Detection
☐ Missing Object Detection
☐ Virtual Fence

CameraName: CAM2331
Event Time: 2015-06-29 14:29:02
Event Type: General Motion Detec...
Label:
Updated:
Note:

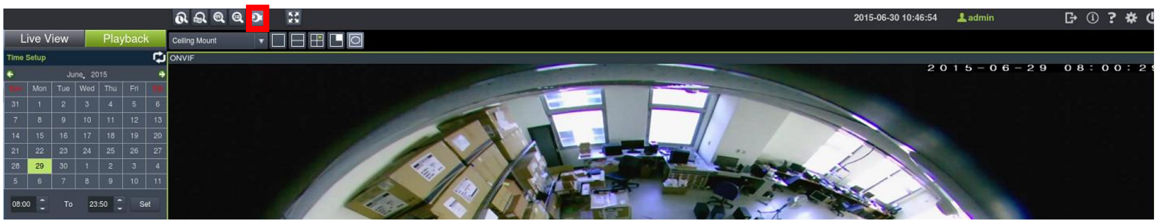
The following functions are available for playback:

📷	Snapshot
🔊	Audio volume
- + 60 Min	Time range can be set when viewing the playback.
⧉ ○ ⧉	Full frame mode

⧉ ● ⧉	Key frame mode
💾	Saves video clips/Exports selected clips
⏮	Clear all the Cue-Ins and Cue-Outs
⇤	Set Cue-In marker for clip start
⇥	Set Cue-In marker for clip end
↻	Automatic reply the clip. (From Cue-in to Cue-Out)
◀	Play backwards
▶	Starts video playback
⏸	Pause video playback
■	Stops video playback.
⏮	Jumps to the previous frame
⏭	Jumps to the next frame
⏪	Jumps to the previous segment
⏩	Jumps to the next segment
- ● + 2X	The play speed can be adjusted from 1x to 8x.

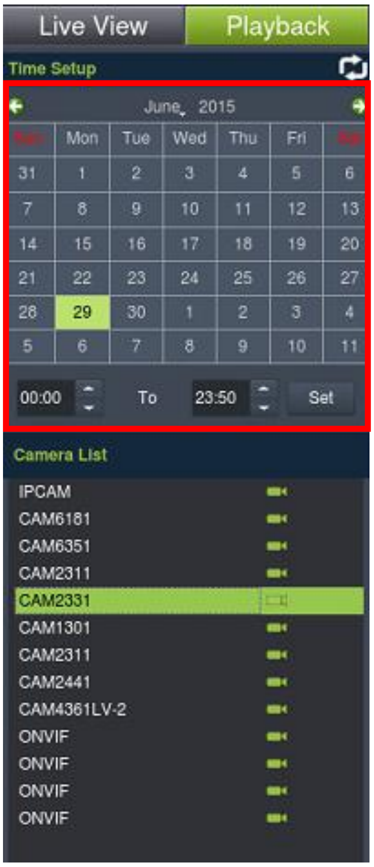
10.6. Fisheye Search

10.6.1. Creating a Fisheye Search



Specified Time

Use the arrows, calendar and time boxes to specify a specific period for search/playback.

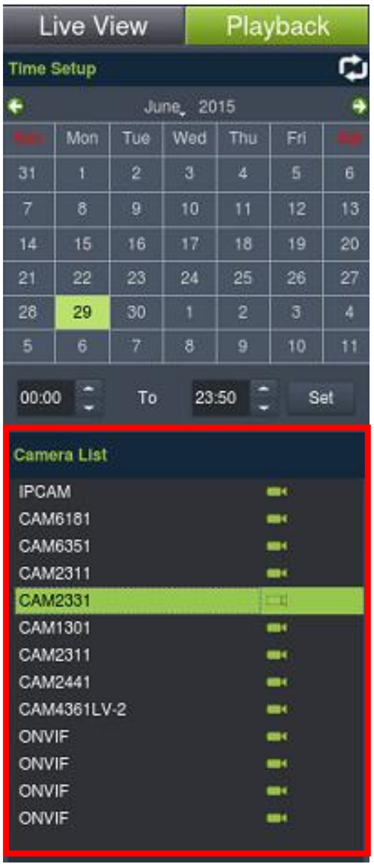


Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

00:00 To 23:50 Set

10.6.2. Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es). Select a fisheye camera for a fisheye search.



June, 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

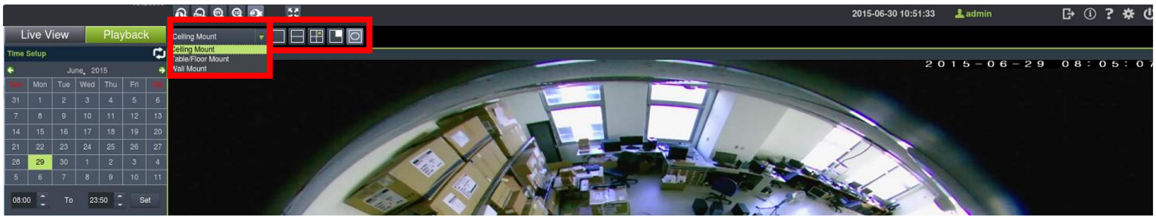
00:00 To 23:50

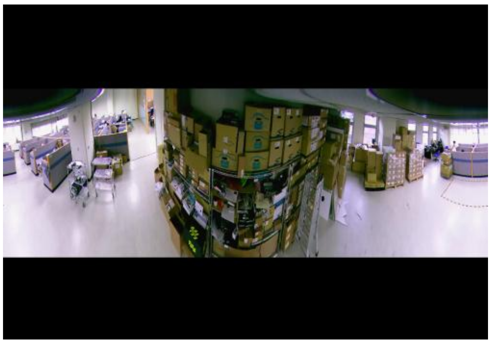
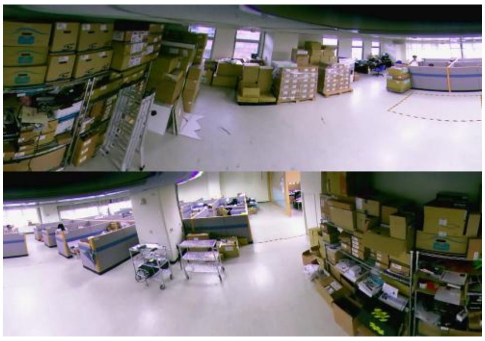
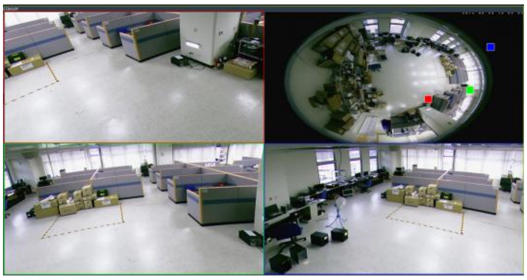
Camera List

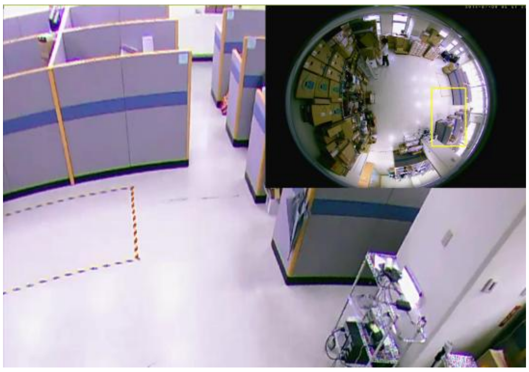
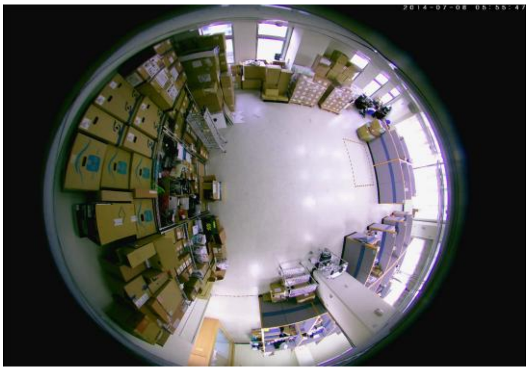
IPCAM
CAM6181
CAM6351
CAM2311
CAM2331
CAM1301
CAM2311
CAM2441
CAM4361LV-2
ONVIF
ONVIF
ONVIF
ONVIF

10.6.3. Use of Various Views Selection

Select according to the way your fisheye is installed to have a best viewing result, Ceiling Mount, Table/Floor Mount or Wall Mount.

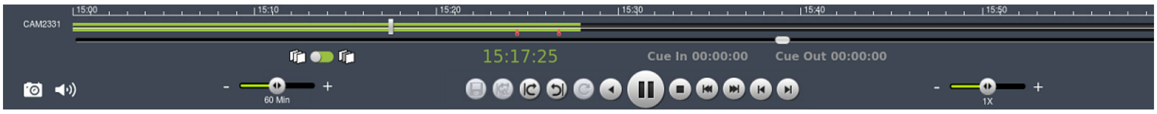


Icon	Description	Reference
□	conventional rectilinear projection, panorama view	
⊟	split-window, horizontal view	
⊞	4 split-windows: 3 enlarged view windows and 1 original fisheye window. Place the different colored boxes in the original fisheye window on the upper right corner to have detailed views projected on the other viewing windows.	

◳	1 enlarged view window and 1 an original fisheye window. Place the colored box in the original fisheye window on the upper right corner to have a detailed view projected.	
⧇	original fisheye view	

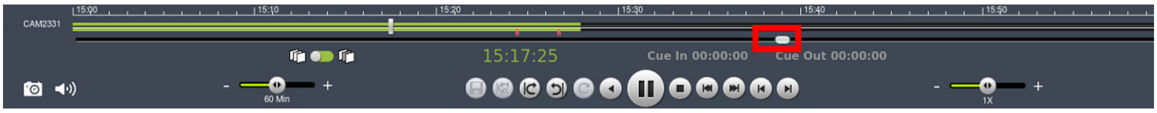
10.6.4. Timeline

After choosing the cameras to view, the timeline for the camera is displayed below the video window.



The timeline window displays a graphic representation of the video information available for the camera on the date and timeframe you have chosen in the *Select Date* window.

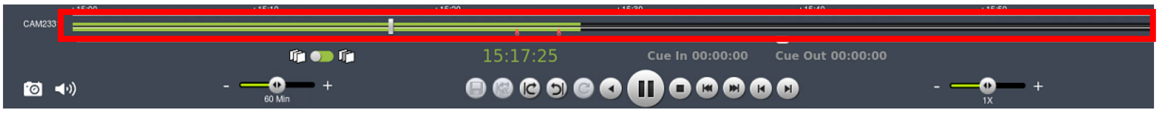
The timeline will, at most, show a period of a little more than 3 hours. If the timeframe that you desire to view is larger than this, the remaining portion of the timeline can be viewed by using the **scrollbar** located beneath the timeline.



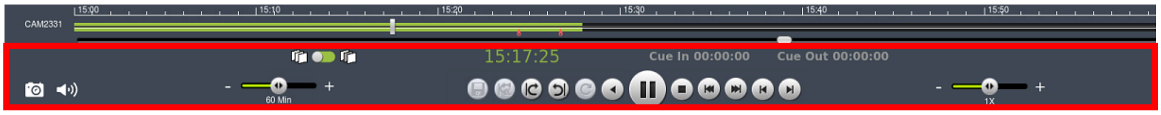
The amount of time displayed in the timeline can also be adjusted using the **slider** located next to the scrollbar. Sliding the indicator toward the right will cause a smaller amount of time to be displayed along the length of the timeline.

10.6.5. Playback

Once a timeline has been loaded, you may choose the point to begin playback. This is done by clicking the **timeline**. After selecting the start point you may start playback.



To start playback of a camera's video feed, ensure that the video is selected. Select feeds by clicking the corresponding pane, timeline, or camera name. Once you have selected a camera, you may use the buttons to control the playback. Playback time is denoted above the control buttons.



Note: The system may take a while to buffer the video before playback starts. A status line above the timeline will indicate portions that have been buffered. Jumping to unbuffered points in the video will cause the system to display an error message.

Clicking on a selected portion of the timeline will cause playback to jump to the point that you have clicked on. You must start playback separately for each feed you wish to view.

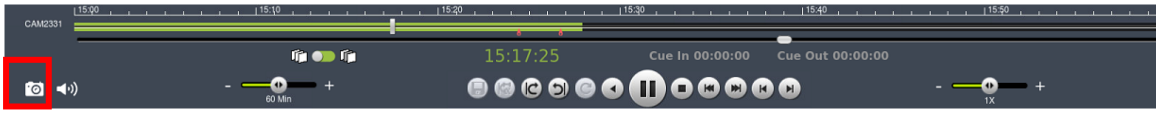
The following table explains the buttons:

📷	Snapshot
🔊	Audio volume
- ━━● + 60 Min	Time range can be set when viewing the playback.
⧉ ○━ ⧉	Full frame mode
⧉ ━○ ⧉	Key frame mode
💾	Saves video clips/Exports selected clips
⏮	Clear all the Cue-Ins and Cue-Outs
⟲	Set Cue-In marker for clip start
⟳	Set Cue-In marker for clip end
↻	Automatic reply the clip. (From Cue-in to Cue-Out)
◀	Play backwards
▶	Starts video playback
⏸	Pause video playback

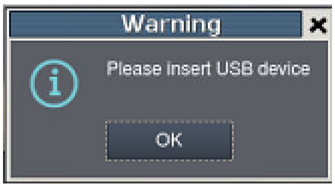
⏹	Stops video playback.
|◀	Jumps to the previous frame
▶|	Jumps to the next frame
⏮	Jumps to the previous segment
⏭	Jumps to the next segment
- ● + 2X	The play speed can be adjusted from 1x to 8x.

Capturing Screenshot

1. Click the **Snapshot** button located in the button area.



The snapshot will be stored in the USB device. Please have your USB device ready.



Warning

Please insert USB device

OK

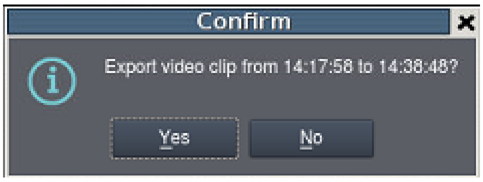
Capturing Video Clip

1. Make sure that the video clip is playing.

2. When the beginning of the segment to be captured is reached, click the **Cue In** button.

3. When the end of the segment to be captured is reached, click the **Cue Out** button.

4. A popup window will appear for confirmation.



Export video clip from 14:17:58 to 14:38:48?

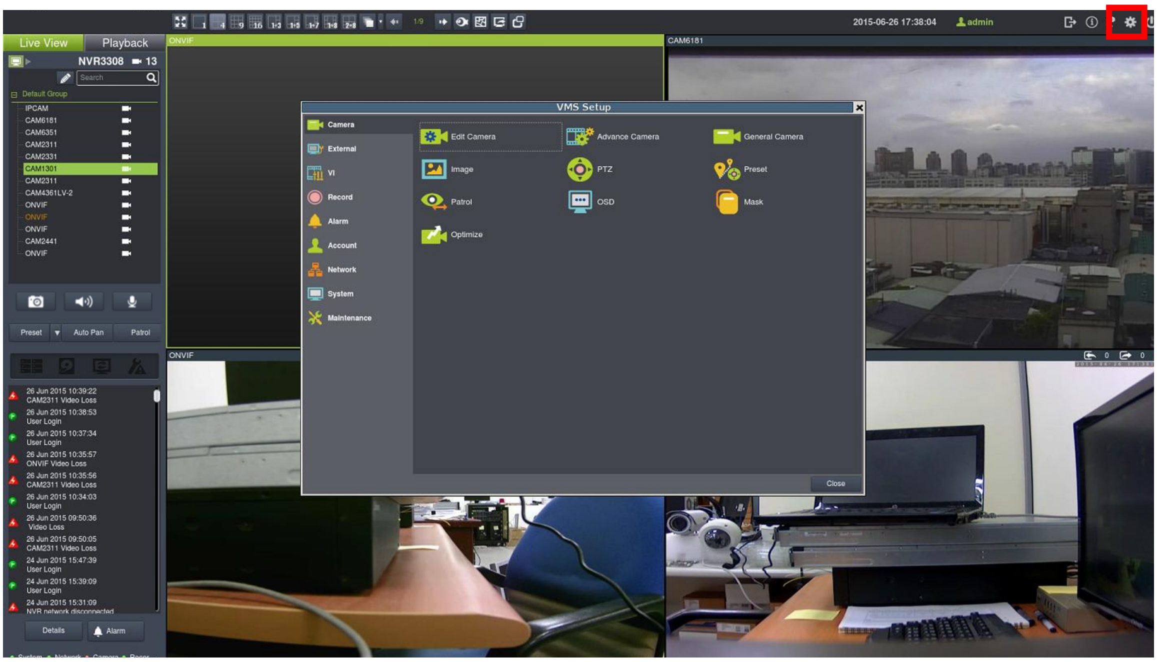
5. Click **Yes** when confirmed. Click **No** and redefine the Cue-In and Cue-Out.

6. The video will be stored in the USB device. Please have your USB device ready.

Chapter 11. VMS Setup

11.1. Camera

Click ⚙ to bring out **VMS Setup** window and select **Camera** to set the camera related settings.



```
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login
26 Jun 2015 09:50:36
 Video Loss
26 Jun 2015 09:50:05
CAM2311 Video Loss
24 Jun 2015 15:47:39
User Login
24 Jun 2015 15:39:09
User Login
24 Jun 2015 15:31:09
NVR network disconnected
```

11.1.1. Edit Camera

The Edit Camera allows you to configure camera settings such as camera vendor, model and permission to access the cameras. See Chapter 8.2.2. *Edit Camera* for more details.

11.1.2. Advanced Camera

Advanced Camera allows you to configure the encoding method, resolution, maximum frame filter and the quality. See Chapter 8.3.2 *Advanced Video Settings* for more details.

11.1.3. General Camera

General Camera allows you to configure the camera connection. See Chapter 8.2.1 *General Camera Settings* for more details.

11.1.4. Image

Image allows you to configure the camera image quality. See Chapter 8.3.1 *Camera Image* for more details.

11.1.5. PTZ

PTZ allows you to configure the PTZ cameras. See Chapter 8.5 *PTZ Settings* for more details.

11.1.6. Preset

Preset allows you to configure the PTZ presets. See Chapter 8.5.2 *PTZ Preset Settings* for more details.

11.1.7. Patrol

Patrol allows you to configure the PTZ patrol. See Chapter 8.5.3 *PTZ Patrol Settings* for more details.

11.1.8. OSD

OSD allows you to configure the OSD overlay, such as camera name, date, time to show on the view. See Chapter 8.2.3 *OSD Settings* for more details.

11.1.9. Mask

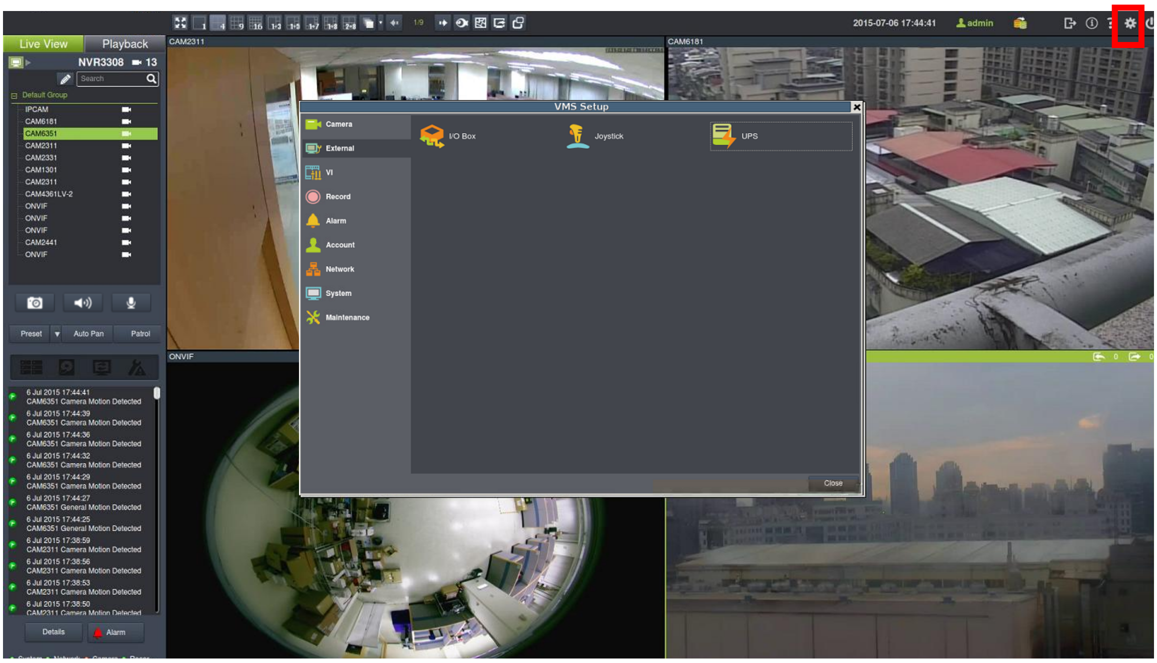
Mask allows you to configure the privacy mask settings. See Chapter 8.2.4 *Privacy Mask Settings* for more details.

11.1.10. Optimize

Optimize allows you to configure the camera to the default settings. See Chapter 8.5.4 Optimize a Camera for more details.

11.2. External

Click to bring out **VMS Setup** window and select **External** to set the external devices related settings.

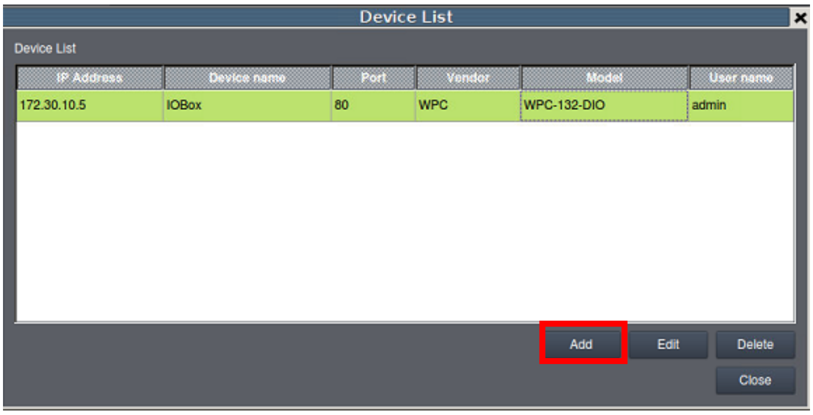


11.2.1. I/O Box

You can add I/O Box to have other external devices connected to the NVR to respond when there triggered.

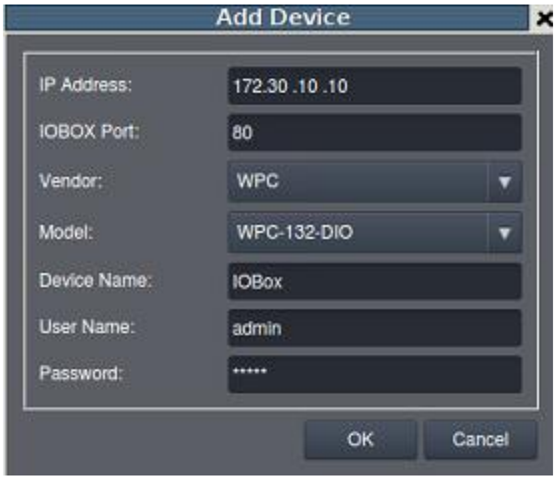
Add

Click I/O box to see this setup page and click **Add**.



Device List

IP Address	Device name	Port	Vendor	Model	User name
172.30.10.5	IOBox	80	WPC	WPC-132-DIO	admin



Add Device

IP Address: 172.30 .10 .10

IOBOX Port: 80

Vendor: WPC

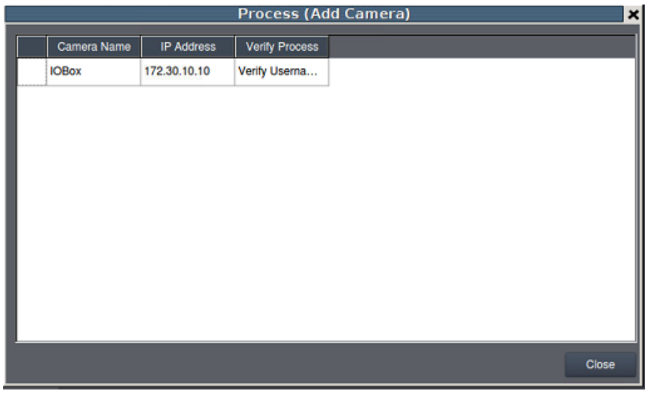
Model: WPC-132-DIO

Device Name: IOBox

User Name: admin

Password: *****

1. In the resulting screen fill out information for the new I/O Box:
   - **IP address**
   - **I/O Box Port**
   - **Vendor:** select from the drop-down list
   - **Model:** select from the drop-down list
   - **Device Name:** create a name for this device
   - **User Name:** input the username
   - **Password:** input the password
2. Click **OK** to add the new I/O Box.



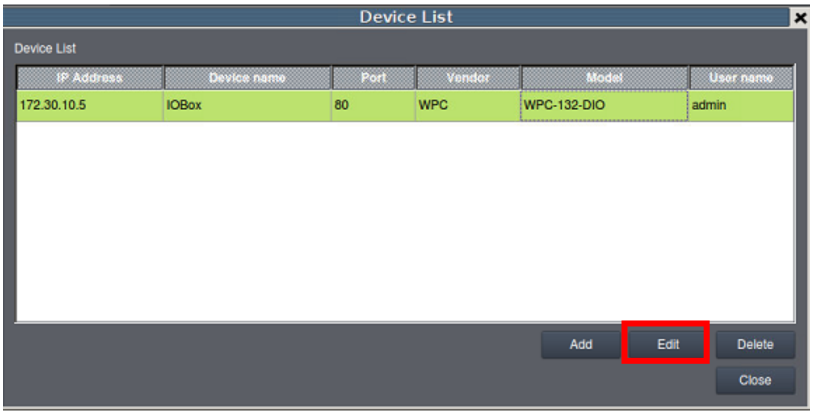
Process (Add Camera)

	Camera Name	IP Address	Verify Process
	IOBox	172.30.10.10	Verify Userna...

3. After verification, the added I/O box will be shown on the list.

Edit

Click I/O box to see this setup page and click **Edit**.

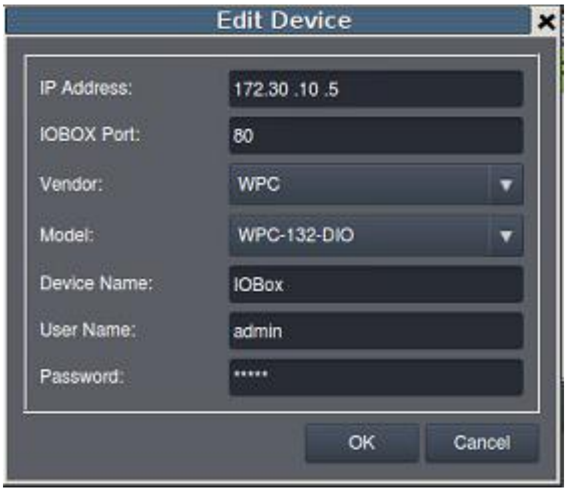


Device List

Device List

IP Address	Device name	Port	Vendor	Model	User name
172.30.10.5	IOBox	80	WPC	WPC-132-DIO	admin

The editing page appears.



Edit Device

IP Address: 172.30 .10 .5

IOBOX Port: 80

Vendor: WPC

Model: WPC-132-DIO

Device Name: IOBox

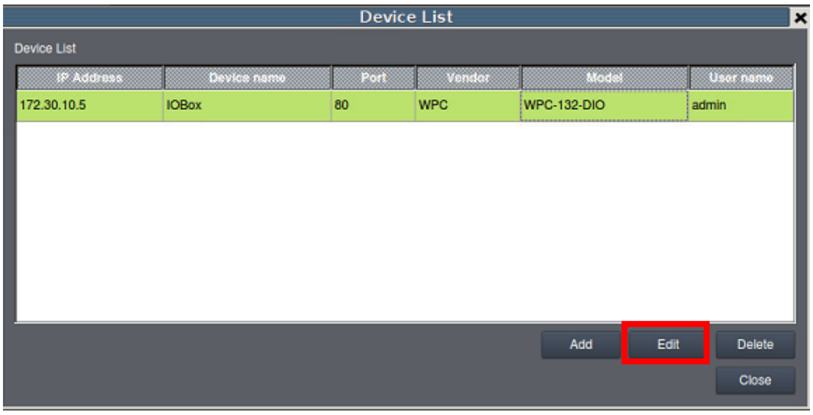
User Name: admin

Password: *****

1. In the resulting screen edit information for the selected I/O Box:
   - **IP address**
   - **I/O Box Port**
   - **Vendor:** select from the drop-down list
   - **Model:** select from the drop-down list
   - **Device Name:** create a name for this device
   - **User Name:** input the username
   - **Password:** input the password
2. Click **OK** to complete the editing.
3. After verification, the edited I/O box will be shown on the list.

Delete

Click I/O box to see this setup page and select the I/O box you'd like to delete and then click **Delete**.



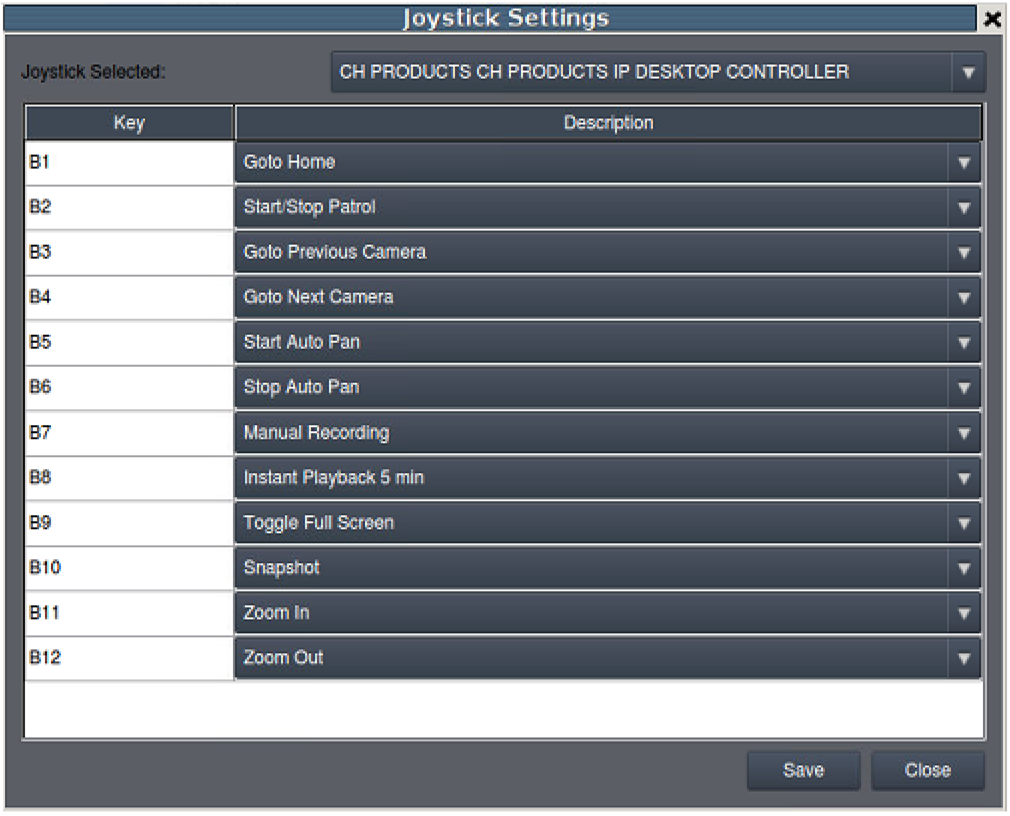
Device List

Device List

IP Address	Device name	Port	Vendor	Model	User name
172.30.10.5	IOBox	80	WPC	WPC-132-DIO	admin

11.2.2. Joystick

CH Products IP Desktop USB Joystick is supported for PTZ camera control. Connect the joystick controller to the USB port. The *Joystick Settings* Window will prompt after clicking **Joystick**. In this window, functions of each button are listed.



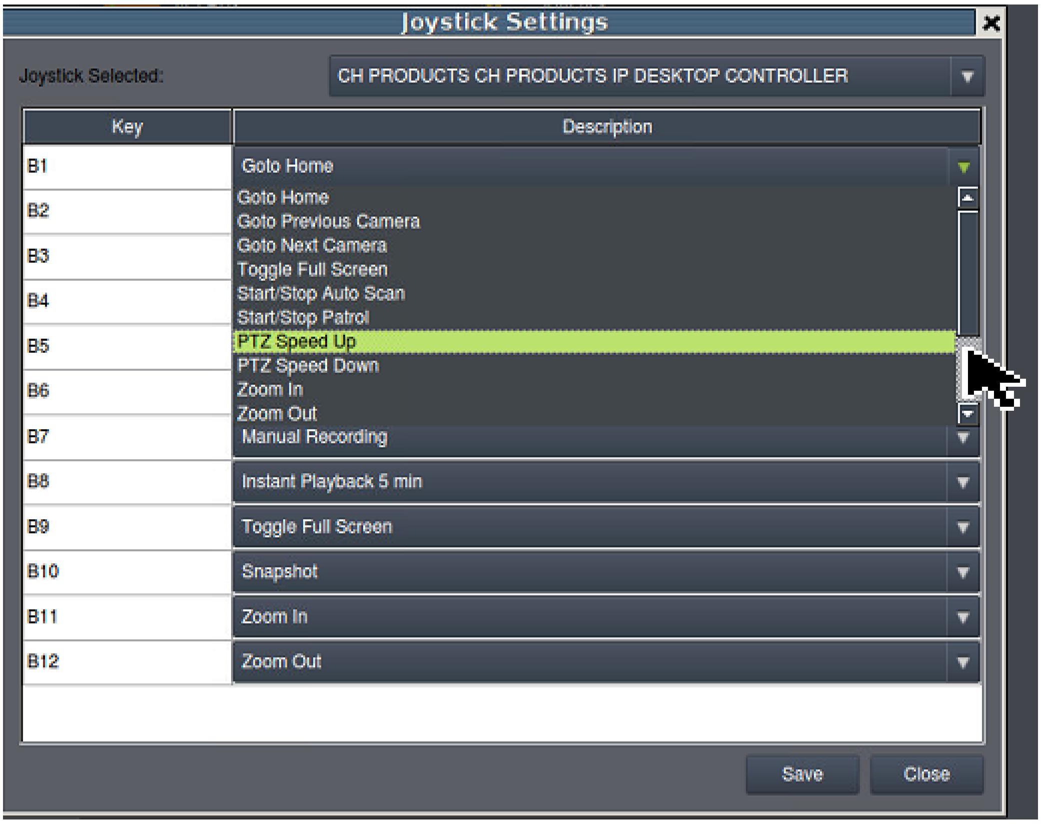
Joystick Settings

Joystick Selected: CH PRODUCTS CH PRODUCTS IP DESKTOP CONTROLLER

Key	Description
B1	Goto Home
B2	Start/Stop Patrol
B3	Goto Previous Camera
B4	Goto Next Camera
B5	Start Auto Pan
B6	Stop Auto Pan
B7	Manual Recording
B8	Instant Playback 5 min
B9	Toggle Full Screen
B10	Snapshot
B11	Zoom In
B12	Zoom Out

Button Number	Function
1	Resets all the settings, including page auto-flipping and different screen divisions.
2	Switches on/off the functionality of switching between preset viewpoints.
3	Goes to the view of the previous camera.
4	Goes to the view of the next camera.
5	Starts auto pan.
6.	Stops auto pan.
7	Manually records the video streams.
8	Pops up an instant playback for five minutes.
9	Brings up the full screen view.
10	Captures a snapshot.
11	Increase the zoom distance.
12	Decrease the zoom distance.

You may reset the functions by choosing within the dropdown list.



Joystick Settings

Joystick Selected: CH PRODUCTS CH PRODUCTS IP DESKTOP CONTROLLER

Key	Description
B1	Goto Home
B2	
B3	
B4	
B5	
B6	
B7	Manual Recording
B8	Instant Playback 5 min
B9	Toggle Full Screen
B10	Snapshot
B11	Zoom In
B12	Zoom Out

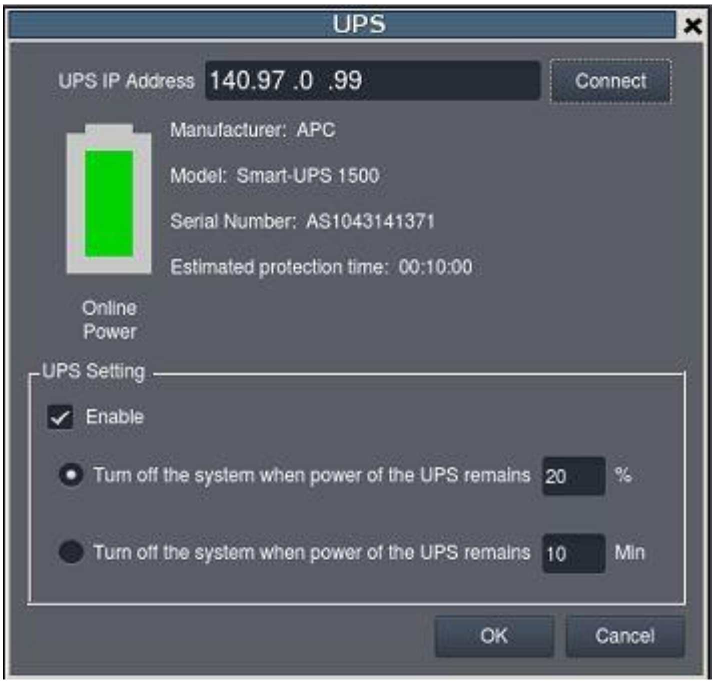
11.2.3. UPS

The system can connect to an UPS (Uninterruptible Power Supply) device to ensure continuous recording and survive power outages. Connect the UPS device to the USB port and input the required UPS IP Address and click **Connect**. Once the UPS device is connected successfully, the manufacture, the model, the serial number, and the estimated protection time will be shown.

UPS settings

Click enable and select one of the following options.

- Turn off the system when power of the UPS remains XX %. (define the percentage)
- Turn off the system when power of the UPS remains XX min. (define the time)



UPS

UPS IP Address 140.97 .0 .99

Manufacturer: APC

Model: Smart-UPS 1500

Serial Number: AS1043141371

Estimated protection time: 00:10:00

Online Power

UPS Setting

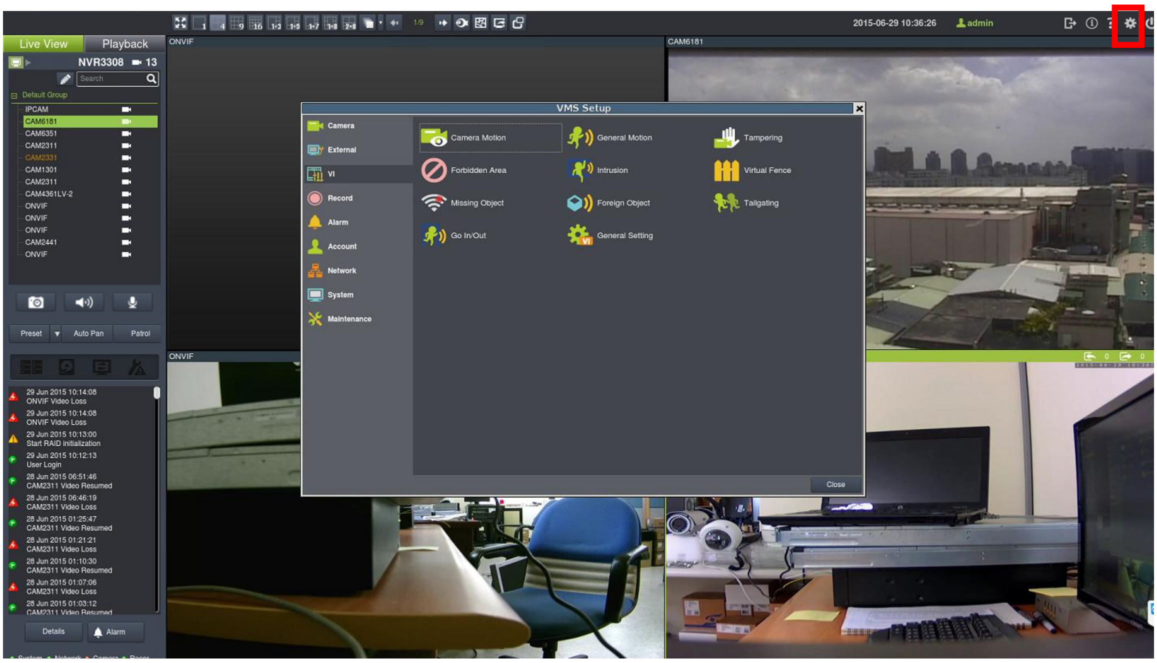
☑ Enable

◉ Turn off the system when power of the UPS remains 20 %

○ Turn off the system when power of the UPS remains 10 Min

11.3. VI

Click ⚙ to bring out **VMS Setup** window and select **VI** to set the VI related settings.



```
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
28 Jun 2015 01:07:06
CAM2311 Video Loss
28 Jun 2015 01:03:12
CAM2311 Video Resumed
```

11.3.1. Camera Motion Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas. See Chapter 8.4.1. *Camera Motion Detection* for more details.

11.3.2. General Motion Detection

Automatically detect the moving target entering the security area. When it moves, an alarm will be triggered. See Chapter 8.4.2 *General Motion Detection* for more details.

11.3.3. Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected. See Chapter 8.4.3 *Tampering Detection* for more details.

11.3.4. Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas. See Chapter 8.4.4 *Forbidden Area Detection* for more details.

11.3.5. Intrusion Detection

Intrusion detection involves using the software to analyze the video feed and detect intrusion larger than a certain size. See Chapter 8.4.5 *Intrusion Detection* for more details.

11.3.6. Virtual Fence Detection

Virtual fence involves using the software to create a fence-crossing detection of the demanding object. See Chapter 8.4.6 *Virtual Fence Detection* for more details.

11.3.7. Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size. See Chapter 8.4.7 *Missing Object Detection* for more details.

11.3.8. Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong. See Chapter 8.4.8 *Virtual Foreign Object Detection* for more details.

11.3.9. Tailgating Detection

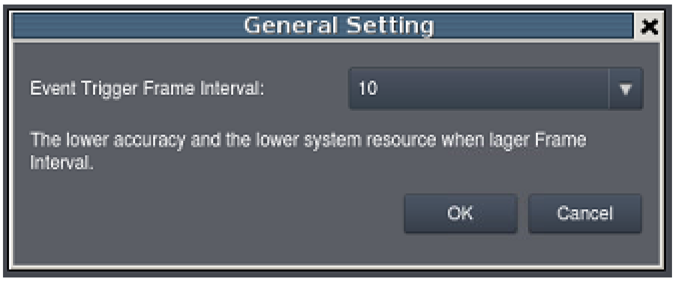
Tailgating detection involves using the software to analyze the video feed and detect a tailgating object crossing over the restricted area. See Chapter 8.4.9 *Tailgating Detection* for more details.

11.3.10. Go In/Out Detection

Go In/Out detection involves using the software to analyze the video feed and detect a go in/out object crossing over the restricted area. See Chapter 8.4.10 *Go In/Out Detection* for more details.

11.3.11. General Setting

Set the frame interval here. The system loading will increase as the frame interval increases.



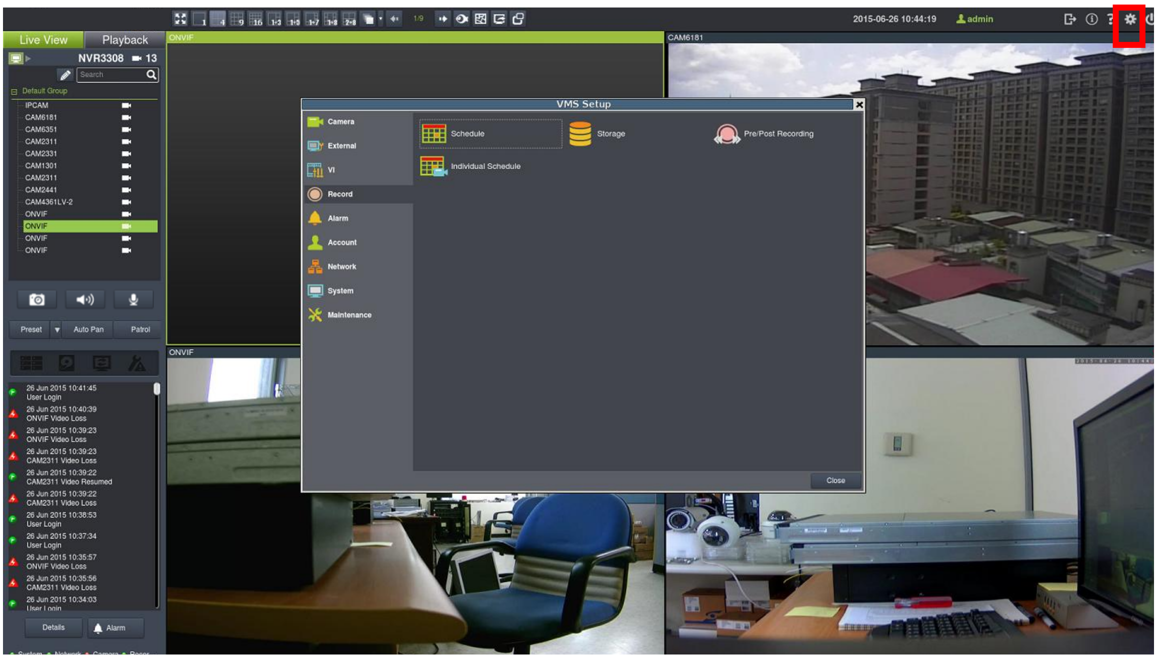
General Setting

Event Trigger Frame Interval: 10

The lower accuracy and the lower system resource when lager Frame Interval.

11.4. Recording

Click ⚙ to bring out **VMS Setup** window and select **Record** to set the recording related settings.



26 Jun 2015 10:41:45
User Login
26 Jun 2015 10:40:39
ONVIF Video Loss
26 Jun 2015 10:39:23
ONVIF Video Loss
26 Jun 2015 10:39:23
CAM2311 Video Loss
26 Jun 2015 10:39:22
CAM2311 Video Resumed
26 Jun 2015 10:39:22
CAM2311 Video Loss
26 Jun 2015 10:38:53
User Login
26 Jun 2015 10:37:34
User Login
26 Jun 2015 10:35:57
ONVIF Video Loss
26 Jun 2015 10:35:56
CAM2311 Video Loss
26 Jun 2015 10:34:03
User Login

11.4.1. Schedule

A Recording Schedule can be created to apply to an entire Server. See Chapter 7.1.3 *Scheduling Recording* for more details.

11.4.2. Storage

Opens the Storage Manager that allows you to configure storage settings. See Chapter 7.1.4. *Storage Management* for more details.

11.4.3. Pre/Post Recording

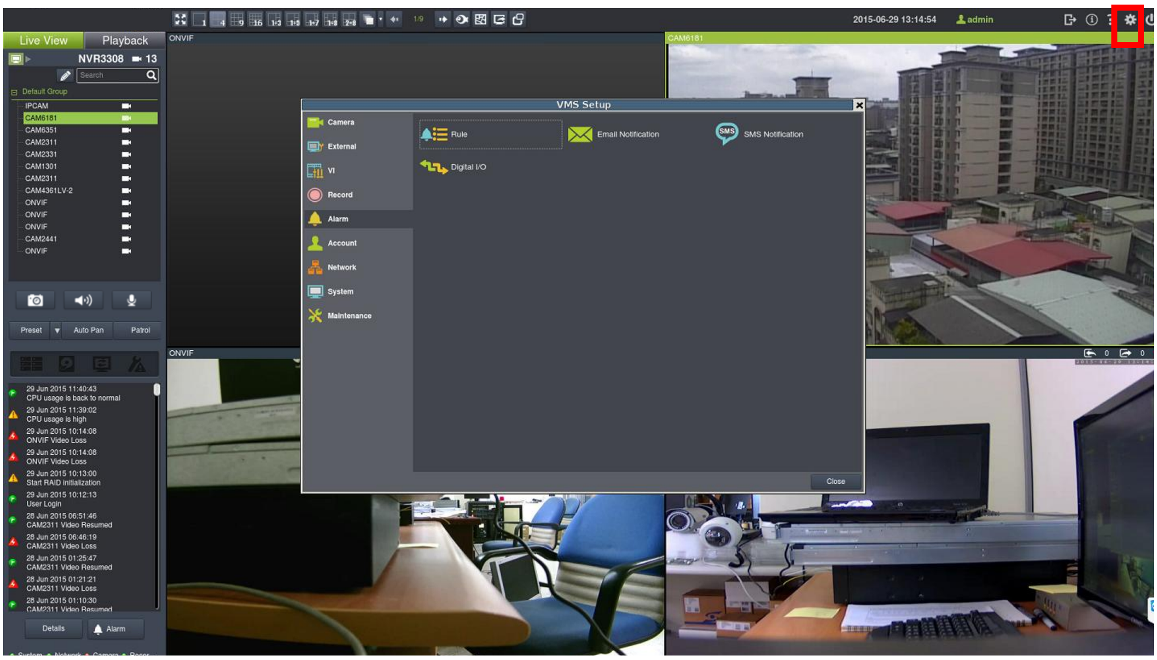
The Server can trace back and preserve video/images from several minutes before and after the occurrence of an alarm. See Chapter 7.1.5 *Pre/Post Recording* for more details.

11.4.4. Individual Schedule

A Recording Schedule can be created to apply to a specific camera. See Chapter 7.1.6 *Individual Schedule* for more details.

11.5. Alarm

Click ⚙ to bring out **VMS Setup** window and select **Alarm** to set the alarm related settings.



```
29 Jun 2015 11:40:43
CPU usage is back to normal
29 Jun 2015 11:39:02
CPU usage is high
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:14:08
ONVIF Video Loss
29 Jun 2015 10:13:00
Start RAID initialization
29 Jun 2015 10:12:13
User Login
28 Jun 2015 06:51:46
CAM2311 Video Resumed
28 Jun 2015 06:46:19
CAM2311 Video Loss
28 Jun 2015 01:25:47
CAM2311 Video Resumed
28 Jun 2015 01:21:21
CAM2311 Video Loss
28 Jun 2015 01:10:30
CAM2311 Video Resumed
```

11.5.1. Rule

In the Alarm Rules, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. See Chapter 9.1. *Alarm Rules* for more details.

11.5.2. Email Notification

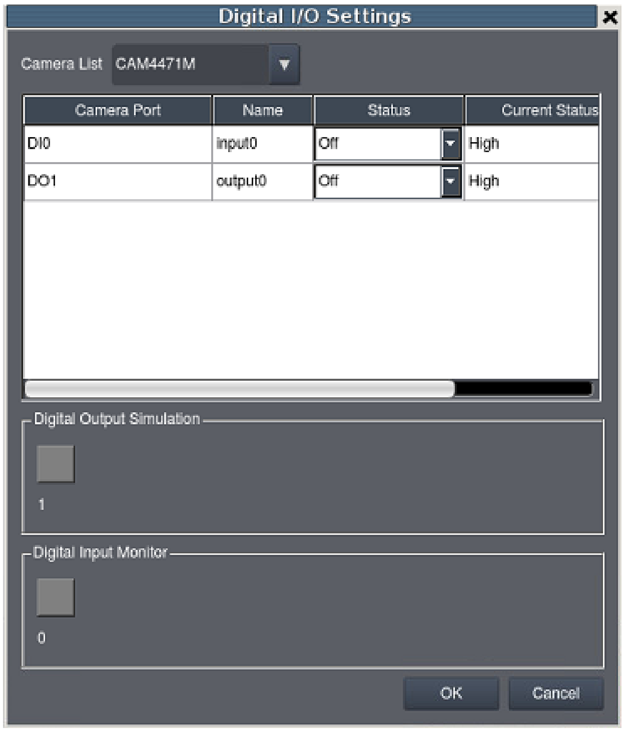
When the alarm is triggered, an E-Mail will be sent. See Chapter 9.1.1. *Adding an Alarm Rule* for more details.

11.5.3. SMS Notification

Configures the SMS setting. See Chapter 9.1.1. *Adding an Alarm Rule* for more details.

11.5.4. Digital I/O Settings

Allows you to configure digital I/O port settings.

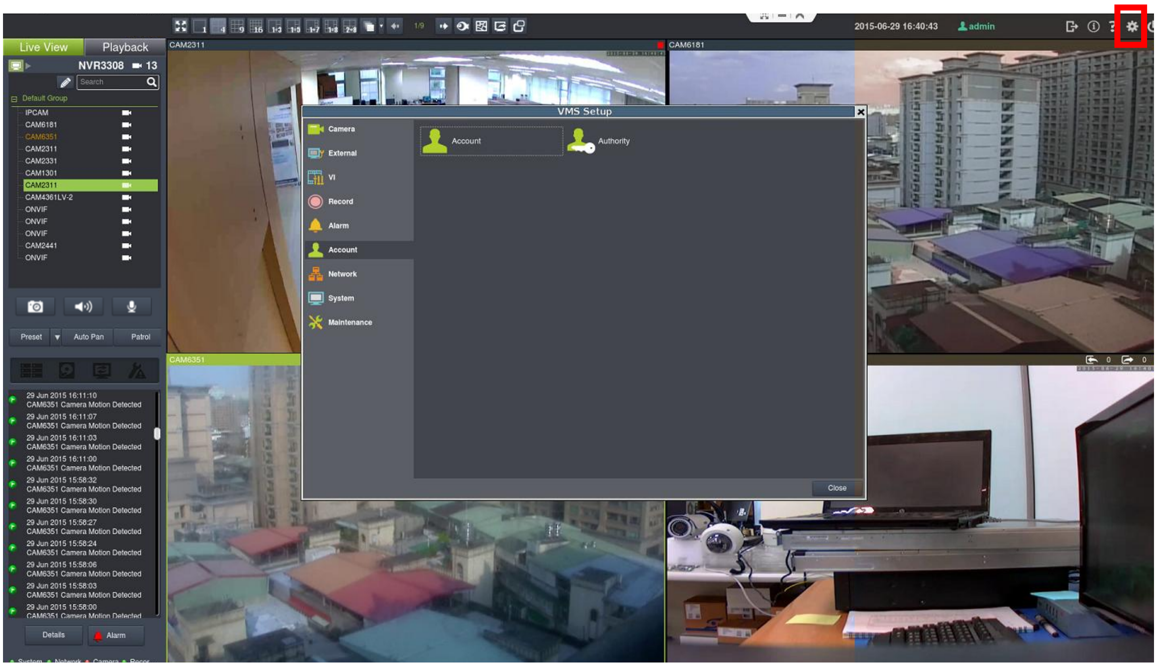


Camera List: CAM4471M

Camera Port	Name	Status	Current Status
DI0	input0	Off	High
DO1	output0	Off	High

11.6. Account

Click ⚙ to bring out **VMS Setup** window and select **Account** to set the account related settings. In this session, accounts and their authorities can be edited, added, and deleted.

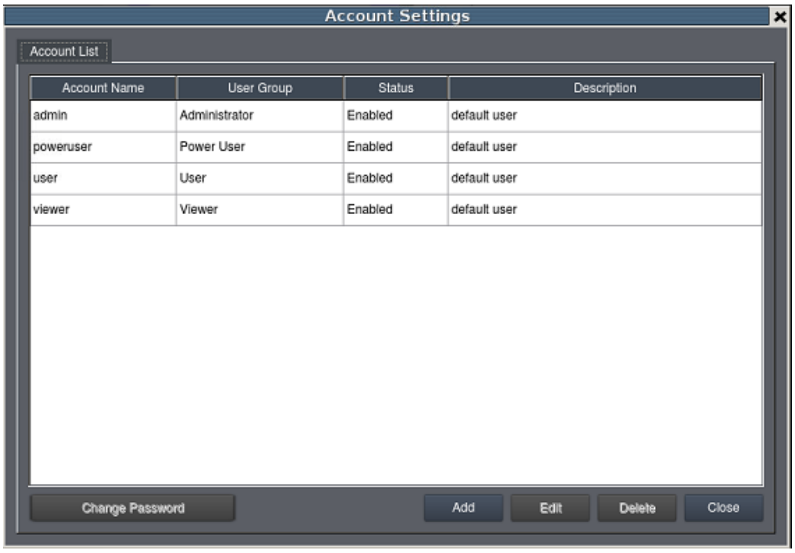


```
29 Jun 2015 16:11:10
CAM6351 Camera Motion Detected
29 Jun 2015 16:11:07
CAM6351 Camera Motion Detected
29 Jun 2015 16:11:03
CAM6351 Camera Motion Detected
29 Jun 2015 16:11:00
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:32
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:30
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:27
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:24
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:06
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:03
CAM6351 Camera Motion Detected
29 Jun 2015 15:58:00
CAM6351 Camera Motion Detected
```

11.6.1. Accounts

The *Account List* provides the following information about each account:

- **Account Name**
- **User Group** - Type for this user.
- **Status** - This shows if the user is disabled or enabled.
- **Description** - A simple description of the user.



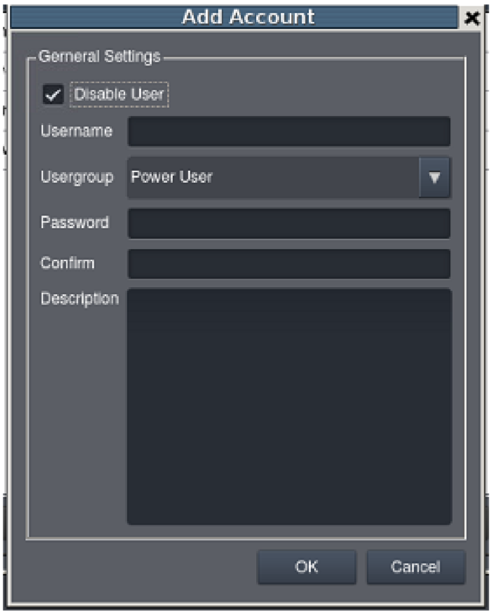
Account Settings

Account List

Account Name	User Group	Status	Description
admin	Administrator	Enabled	default user
poweruser	Power User	Enabled	default user
user	User	Enabled	default user
viewer	Viewer	Enabled	default user

Add Account

To add an account to the domain:



Add Account

Gerneral Settings

☑ Disable User

Username

Usergroup: Power User

Password

Confirm

Description

4. Click the **Add** button at the bottom of the *Account List* screen.

5. In the resulting screen fill out information for the new account:
   - **Username**
   - **User Group -** Select a user type for this user. There are four options:
     - **Administrator** – This group has complete management privileges, including account and VMS/Server management rights.
     - **Power User** – This group has complete account management rights, but does not have many VMS/Server configuration rights.
     - **User** – This group has no configuration rights and limited VMS/Server performance statistics.
     - **Viewer** – This group is limited only to viewing, and has no access to configuration or performance statistics.
   - **Password / Confirm Password** – The password must be typed twice for confirmation purposes.
   - **Description** – A simple description of the new user.

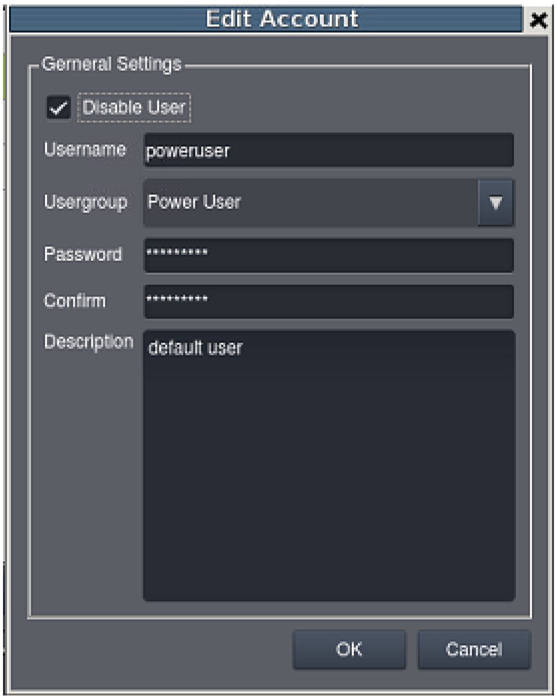
6. Check the **Disable User** box to disable this account.

7. Click **Ok** to add the new account. The account will appear in the *Account List*.

Editing an Account

To edit an account to the domain:

1. Access the *Account List* node in the *VMS Setup*.
2. Select the account that you wish to edit by clicking on the account.



☑ Disable User

Username poweruser

Usergroup Power User ▼

Password *********

Confirm *********

Description default user

3. Click the **Edit** button at the bottom of the *Account List* screen.
4. In the resulting screen change any of the following account information:

- **User Group -** Selects a user type for this user. There are four options:
    - **Administrator** – This group has complete management privileges, including account and VMS/NVR Server management rights.
    - **Power User** – This group has complete account management rights, but does not have many VMS/NVR Server configuration rights.
    - **User -** This group has no configuration rights and limited VMS/Server performance statistics.
    - **Viewer** – This group is limited only to viewing, and has no access to configuration or performance statistics.

- **Password/Confirm Password** – If changed the password must be typed twice for confirmation purposes.
- **Description -** A simple description of the user.

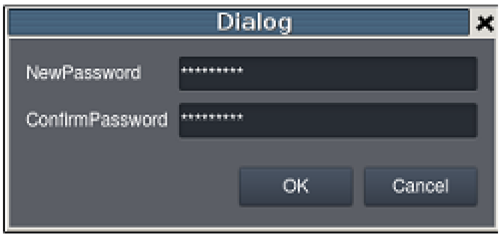
5. If desired check the **Disable User** box to disable this account.

6. Click **Ok** to save the changes to the account. If the account description, user group or status changes, it will be reflected in the *Account List*.

Changing an Account Password

In addition to editing the password from using the *Account List* editing function, the password for the current account can also be changed by clicking the **Change Password** at the lower left corner of *Account List Window*.

This will display a dialog that allows you to enter and confirm a new password.



NewPassword **********

ConfirmPassword **********

Deleting an Account

To delete an account to the domain:

1. Access the *Account List* node in the *VMS Setup*.

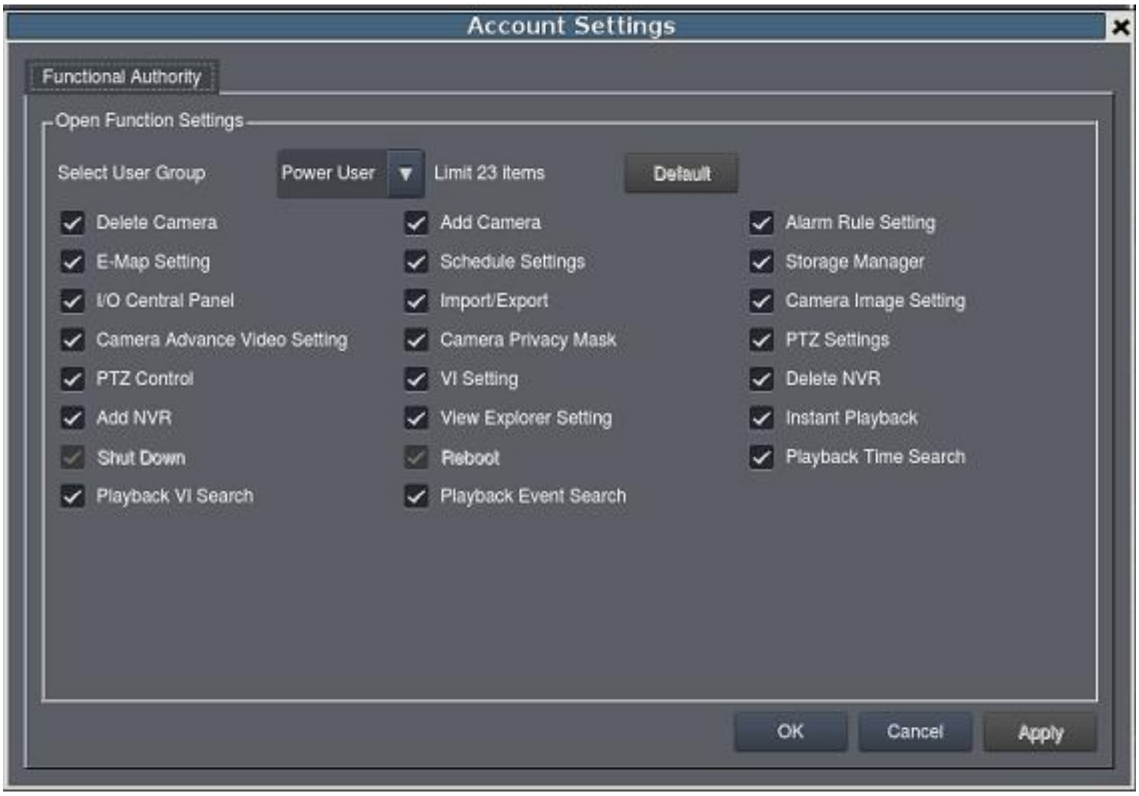
2. Select the account that you wish to delete by clicking on the account.

3. Click the **Delete** button at the bottom of the *Account List* screen.

4. When prompted to confirm deletion click **Yes** to delete the account. The deletion will be reflected in the *Account List*.

> **Note:** The *Admin* account cannot be deleted.

11.6.2. Account Authority Settings



Account Settings

Functional Authority

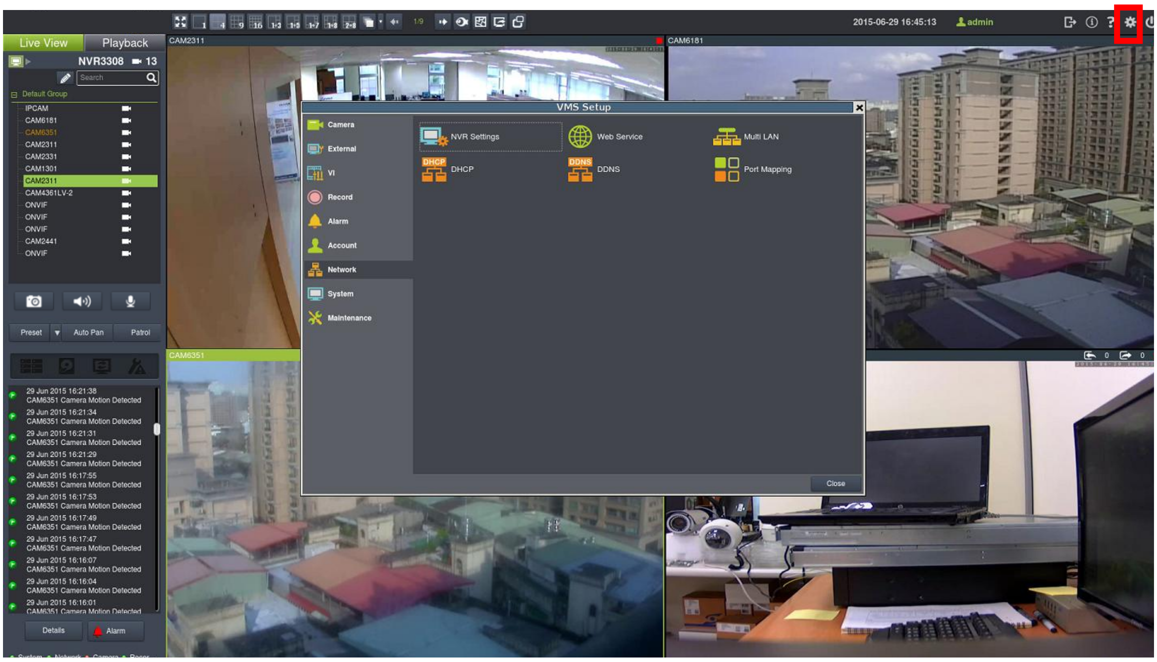
Open Function Settings

Select User Group: Power User ▼ Limit 23 items Default

- ☑ Delete Camera
- ☑ E-Map Setting
- ☑ I/O Central Panel
- ☑ Camera Advance Video Setting
- ☑ PTZ Control
- ☑ Add NVR
- ☑ Shut Down
- ☑ Playback VI Search
- ☑ Add Camera
- ☑ Schedule Settings
- ☑ Import/Export
- ☑ Camera Privacy Mask
- ☑ VI Setting
- ☑ View Explorer Setting
- ☑ Reboot
- ☑ Playback Event Search
- ☑ Alarm Rule Setting
- ☑ Storage Manager
- ☑ Camera Image Setting
- ☑ PTZ Settings
- ☑ Delete NVR
- ☑ Instant Playback
- ☑ Playback Time Search

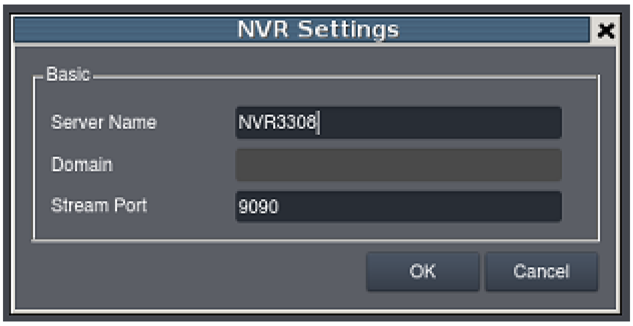
11.7. Network

Click ⚙ to bring out **VMS Setup** window and select **Network** to set the network related settings.



11.7.1. NVR Settings

Users can change both the setting of the stream port and the IP address by editing the Server.



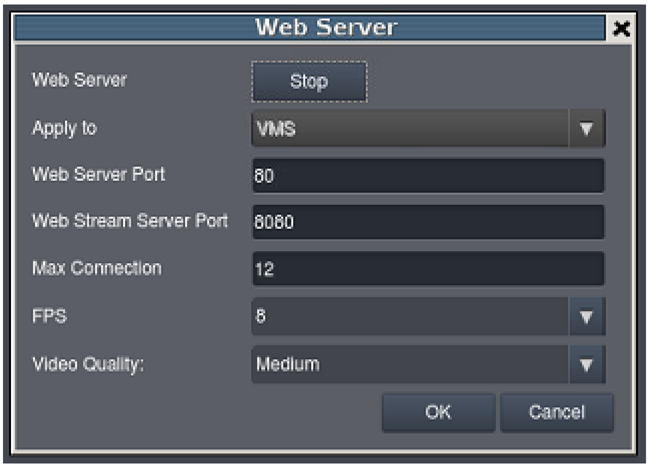
NVR Settings

Basic

Server Name	NVR3308
Domain	
Stream Port	9090

11.7.2. Web Server

For users who want to use the Web Client/Mobile Client, please fill in the following information for the Web Server settings.



Web Server

Web Server: Stop

Apply to: VMS

Web Server Port: 80

Web Stream Server Port: 8080

Max Connection: 12

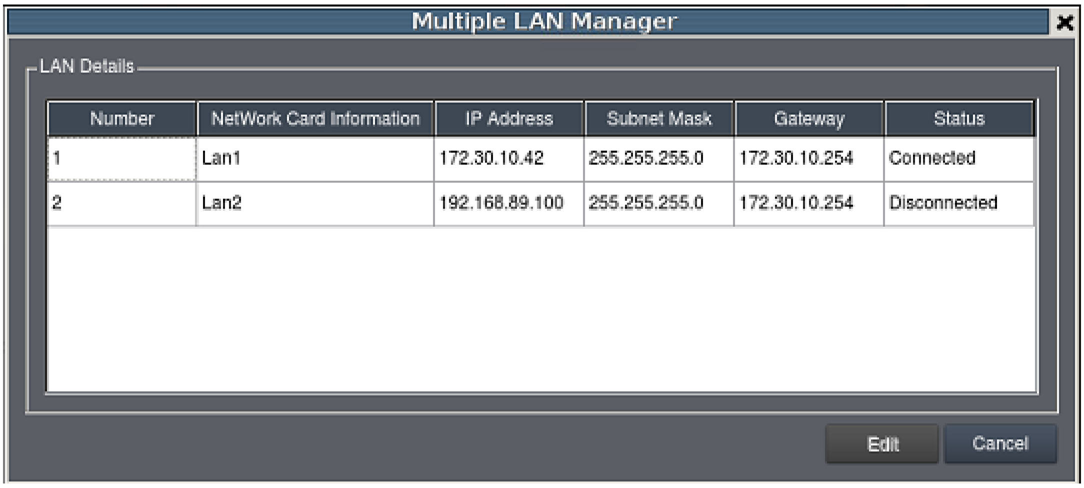
FPS: 8

Video Quality: Medium

Note: (1) User may just keep the default settings in the Web Server. (2) Do not set the Web Server Port as these port numbers – 8080 (Web Stream Port), 9090 (NVR Stream Port), 2809 (NVR Server Login Port), 7735 (TV Wall Port (2.5.0)), 7734, 1024, 9010 (Domain Broadcast Port), 9030 (Domain Client Message Port), 9040 (Domain Console Message Port), 9050 (Domain Local Communication Port), 9020 (Domain Remote Communication Port), 9080 (Domain Local Log Data Download Port), 9081 (Domain Remote Log Data Download Port), 9060 (Domain Local Data Port), 9061 (Domain Remote Data Port), 15507 (Domain Local Log Message Download Port), 15503 (Domain Remote Log Message Download Port), 15501 (Domain Remote Log Upload port), 15505 (Domain Local Log Upload Port), 40000 (NVR Broadcast Port), 50000 (NVR Message Port).

11.7.3. Multiple LAN

Multiple network cards can be supported. Their information is listed as below:

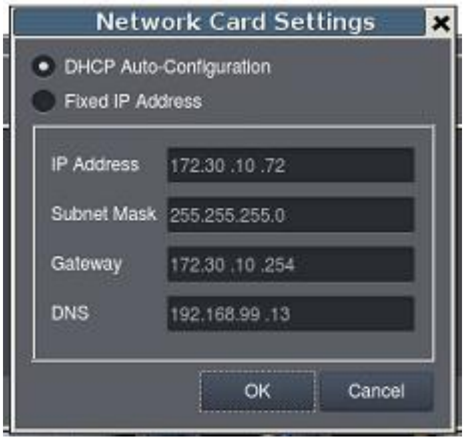


Multiple LAN Manager

LAN Details

Number	NetWork Card Information	IP Address	Subnet Mask	Gateway	Status
1	Lan1	172.30.10.42	255.255.255.0	172.30.10.254	Connected
2	Lan2	192.168.89.100	255.255.255.0	172.30.10.254	Disconnected

Click the “**Edit**” to set the Network Card to DHCP Auto-Configuration or Fixed IP.



Network Card Settings

● DHCP Auto-Configuration

○ Fixed IP Address

IP Address: 172.30 .10 .72

Subnet Mask: 255.255.255.0

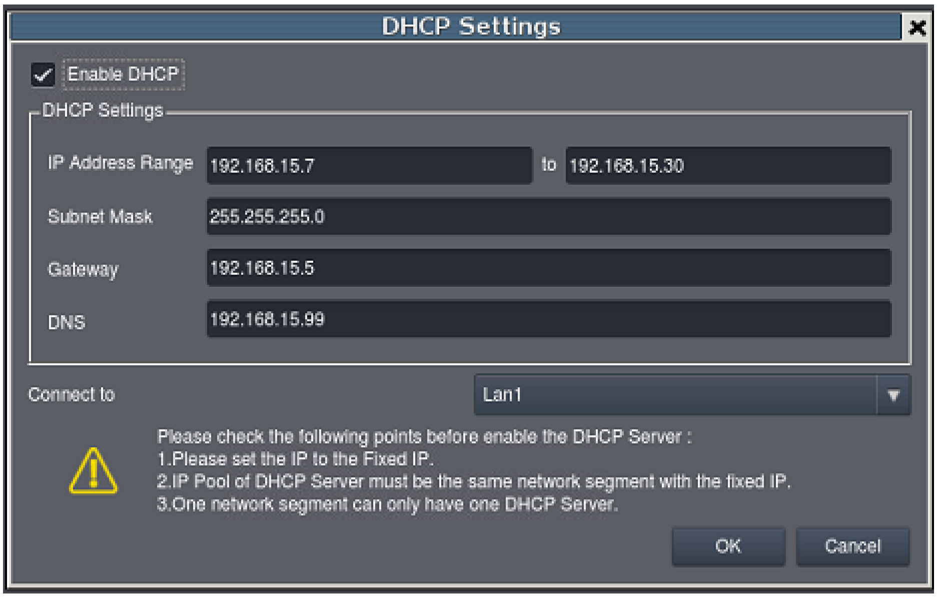
Gateway: 172.30 .10 .254

DNS: 192.168.99 .13

11.7.4. DHCP Settings

The VMS has built in DHCP server functionality. Although this function is disabled by factory default, it should be turned on in the event that there is no DHCP service available. When enabled, the VMS will assume DHCP Server duties and assign addresses within the range specified.

Note: You may skip this step if you have separate DHCP service. Most routing devices will have DHCP capabilities.



DHCP Settings

☑ Enable DHCP

DHCP Settings

IP Address Range: 192.168.15.7 to 192.168.15.30

Subnet Mask: 255.255.255.0

Gateway: 192.168.15.5

DNS: 192.168.15.99

Connect to: Lan1

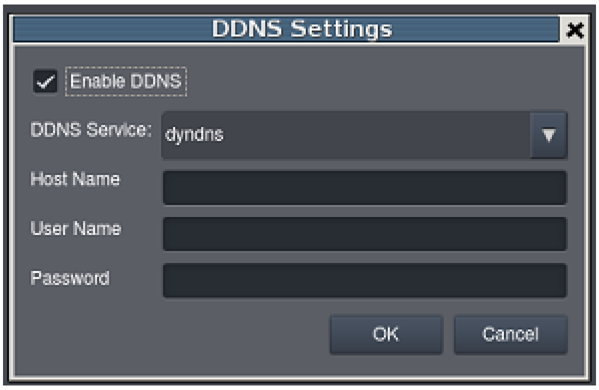
Please check the following points before enable the DHCP Server :
1.Please set the IP to the Fixed IP.
2.IP Pool of DHCP Server must be the same network segment with the fixed IP.
3.One network segment can only have one DHCP Server.

1. Fill in the following information:

   - **IP Address Range -** The range of addresses to be assigned. The first IP address should be lower than the second IP address.
   - **Subnet Mask**
   - **Router** - The router IP
   - **Domain Name** - The DNS IP

Note: The DHCP service should be attached to a network card.

11.7.5. DDNS Setting


DDNS Settings

☑ Enable DDNS

DDNS Service: dyndns

Host Name

User Name

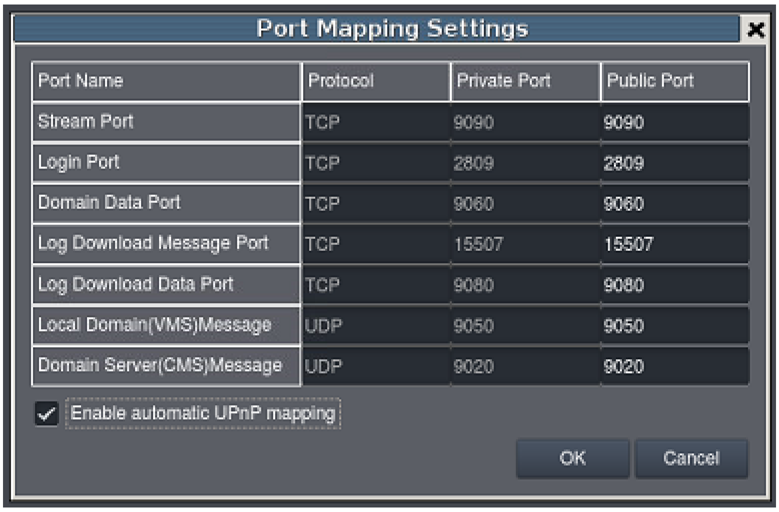
Password

DDNS (Dynamic Domain Name Server) is a protocol that enables the camera to maintain a static connection address, even when its IP changes. Access using this feature is disabled by default.

Connecting using DDNS requires registration on third-party websites for DDNS services. Select desired DDNS service website, check the **Enable DDNS** option, and fill in valid user name and password. You can then access the camera through the registered domain name.

11.7.6. Port Mapping

A *Router Port Mapping* window will prompt for entering port numbers. See Chapter 3.4.1. Port Forwarding for Accessing VMS Server for more details.


Port Mapping Settings

Port Name	Protocol	Private Port	Public Port
Stream Port	TCP	9090	9090
Login Port	TCP	2809	2809
Domain Data Port	TCP	9060	9060
Log Download Message Port	TCP	15507	15507
Log Download Data Port	TCP	9080	9080
Local Domain(VMS)Message	UDP	9050	9050
Domain Server(CMS)Message	UDP	9020	9020

☑ Enable automatic UPnP mapping

Stream Port: 9090
Login: Port: 2809
Doman Data Port: 9060
Log Download Message Port: 15507
Log Download Data Port: 9080

2. Open Ports on the Router
Host Ports: The private ports that the internal VMS/NVR Server use, which are unchangeable.

Global Ports: The public ports for remote clients to connect to the internal VMS/NVR Server. The Global ports are changeable, but the simplest way is to make them the same with the host ports.

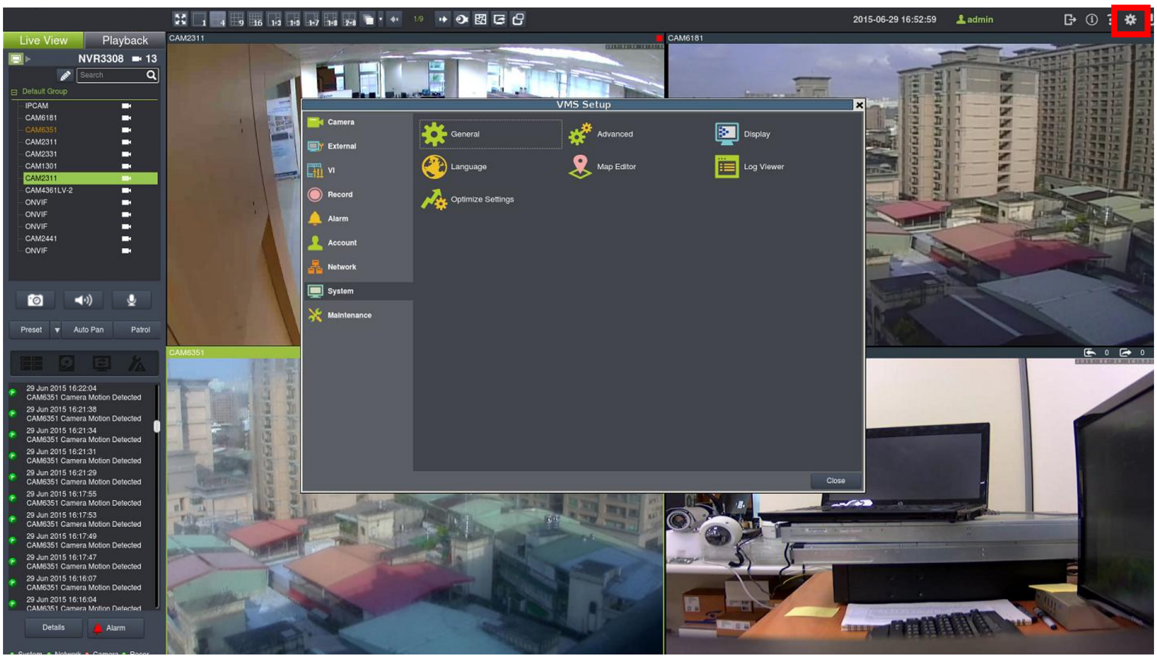
Please open the listed ports on your router:

Port(Host/Global Port)	**Protocol**	**Port Number**
Domain Message Port	UDP	9050
Domain Data Port	TCP	9060
Login Port	TCP	2809
Stream Port	TCP	9090
Log Download Message Port	TCP	15507
Log Download Data Port	TCP	9080

Note: Camera port (default: 80) and stream port (default: 6002) for accessing cameras should be opened while VMS/NVR Server and the cameras and are not in the same LAN.

11.8. System

Click to bring out **VMS Setup** window and select **System** to set the system related settings.

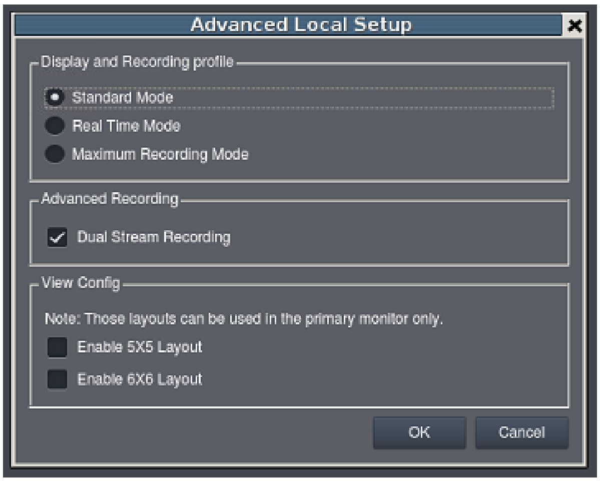


```
29 Jun 2015 16:22:04
CAM6351 Camera Motion Detected
29 Jun 2015 16:21:38
CAM6351 Camera Motion Detected
29 Jun 2015 16:21:34
CAM6351 Camera Motion Detected
29 Jun 2015 16:21:31
CAM6351 Camera Motion Detected
29 Jun 2015 16:21:29
CAM6351 Camera Motion Detected
29 Jun 2015 16:17:55
CAM6351 Camera Motion Detected
29 Jun 2015 16:17:53
CAM6351 Camera Motion Detected
29 Jun 2015 16:17:49
CAM6351 Camera Motion Detected
29 Jun 2015 16:17:47
CAM6351 Camera Motion Detected
29 Jun 2015 16:16:07
CAM6351 Camera Motion Detected
29 Jun 2015 16:16:04
CAM6351 Camera Motion Detected
```

11.8.1. General

Server settings can be configured under the *General Server Settings* menu. See Chapter 7.1.1. *General Server Settings* for more details.

11.8.2. Advanced



Advanced Local Setup

Display and Recording profile

- ● Standard Mode
- ○ Real Time Mode
- ○ Maximum Recording Mode

Advanced Recording

- ☑ Dual Stream Recording

View Config

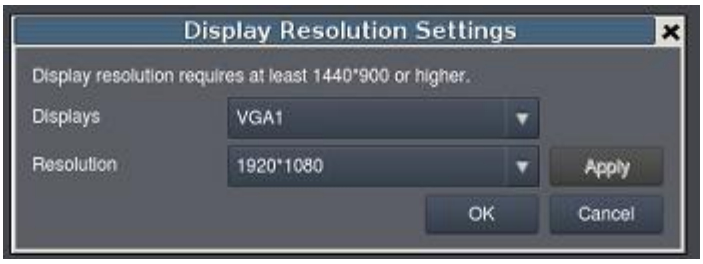
Note: Those layouts can be used in the primary monitor only.

- □ Enable 5X5 Layout
- □ Enable 6X6 Layout

Settings concerning display and recording profile, dual stream recording, and view layout can be configured here.

11.8.3. Display Resolution Settings

Shows the monitor resolution, and allows you to change its setting.



Display Resolution Settings

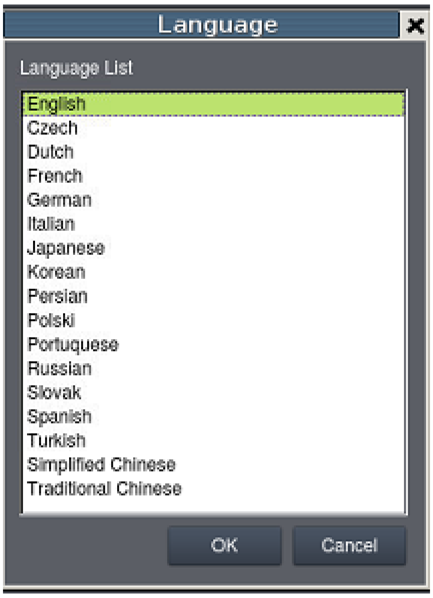
Display resolution requires at least 1440*900 or higher.

Displays: VGA1

Resolution: 1920*1080

11.8.4. Language

NVR 3000 Series supports the following languages: Dutch, English, German, Italian, Japanese, Korean, Persian, Russian, Simplified Chinese, Spanish, Traditional Chinese, and Turkish.



Language

Language List

English
Czech
Dutch
French
German
Italian
Japanese
Korean
Persian
Polski
Portuquese
Russian
Slovak
Spanish
Turkish
Simplified Chinese
Traditional Chinese

11.8.5. Map Editor

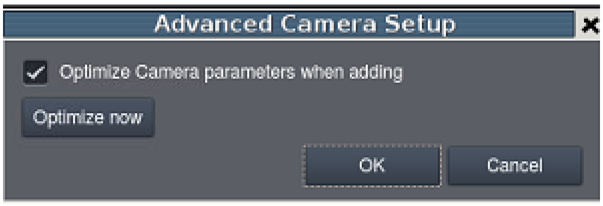
E-map can be configured here. See Chapter 6.2.1. E-map for more details.

11.8.6. Log Viewer

Log can be viewed under the View Log menu. See Chapter 9.2. *Event Log* for more details.

11.8.7. Optimize Settings

Once click on the option "Optimize now", a confirm window will pop up. This action will apply to all cameras connected.

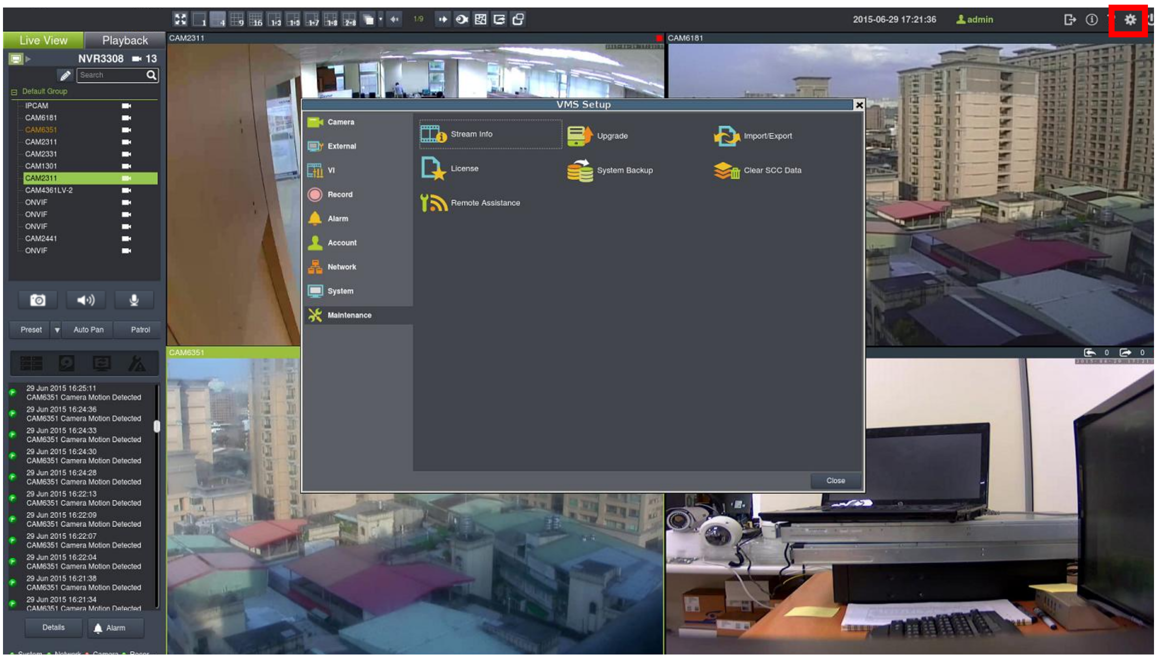


Advanced Camera Setup

☑ Optimize Camera parameters when adding

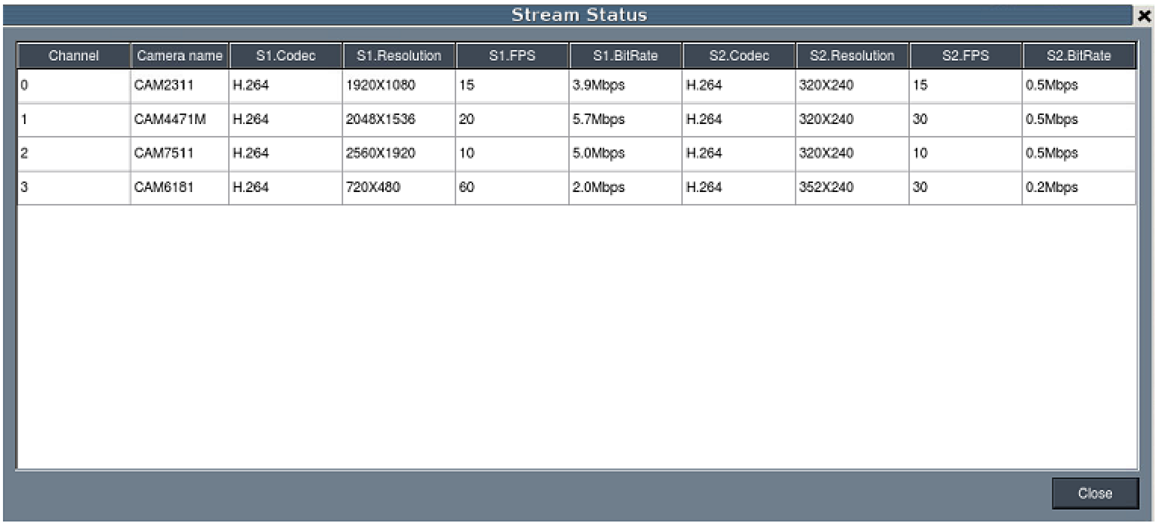
11.9. Maintenance

Click ⚙ to bring out **VMS Setup** window and select **Maintenance** to set the maintenance related settings.



11.9.1. Stream Status

From here you can see all the stream information, such as channel, camera name, codec, resolution, FPS, and bit-rate.

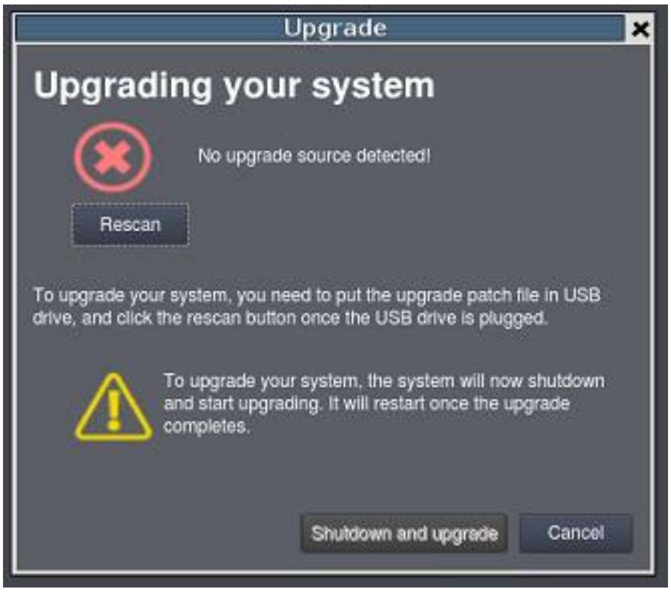

Stream Status

Channel	Camera name	S1.Codec	S1.Resolution	S1.FPS	S1.BitRate	S2.Codec	S2.Resolution	S2.FPS	S2.BitRate
0	CAM2311	H.264	1920X1080	15	3.9Mbps	H.264	320X240	15	0.5Mbps
1	CAM4471M	H.264	2048X1536	20	5.7Mbps	H.264	320X240	30	0.5Mbps
2	CAM7511	H.264	2560X1920	10	5.0Mbps	H.264	320X240	10	0.5Mbps
3	CAM6181	H.264	720X480	60	2.0Mbps	H.264	352X240	30	0.2Mbps

11.9.2. Upgrade

Upgrading can be done here. Have the USB with the upgrade patch file connected to the system. And then click the Rescan button. The upgrade patch file in the USB will be read and the upgrading can begin.

Once the upgrade is done, the system will reboot to update the settings.



Upgrade

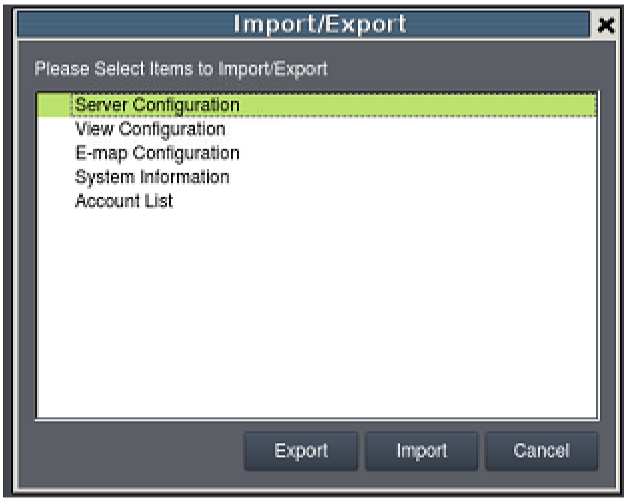
Upgrading your system

No upgrade source detected!

To upgrade your system, you need to put the upgrade patch file in USB drive, and click the rescan button once the USB drive is plugged.

To upgrade your system, the system will now shutdown and start upgrading. It will restart once the upgrade completes.

11.9.3. Import/Export



Import/Export

Please Select Items to Import/Export

- Server Configuration
- View Configuration
- E-map Configuration
- System Information
- Account List

The following types of configuration/setup files can be imported/exported to the Server:

- **Server Configuration**
- **View Configuration**
- **E-map Configuration**
- **System Information**
- **Account List**

Importing Parameters

To import parameters into the Server:

1. Select the item that you wish to import by clicking on the item type.
2. Click the **Import** button. A windows explorer dialog will appear.
3. Select the file to import from the file explorer, and click **Open** to import the file.
4. Click **OK** to confirm import. The Server will require a restart before imported configurations and files are applied.

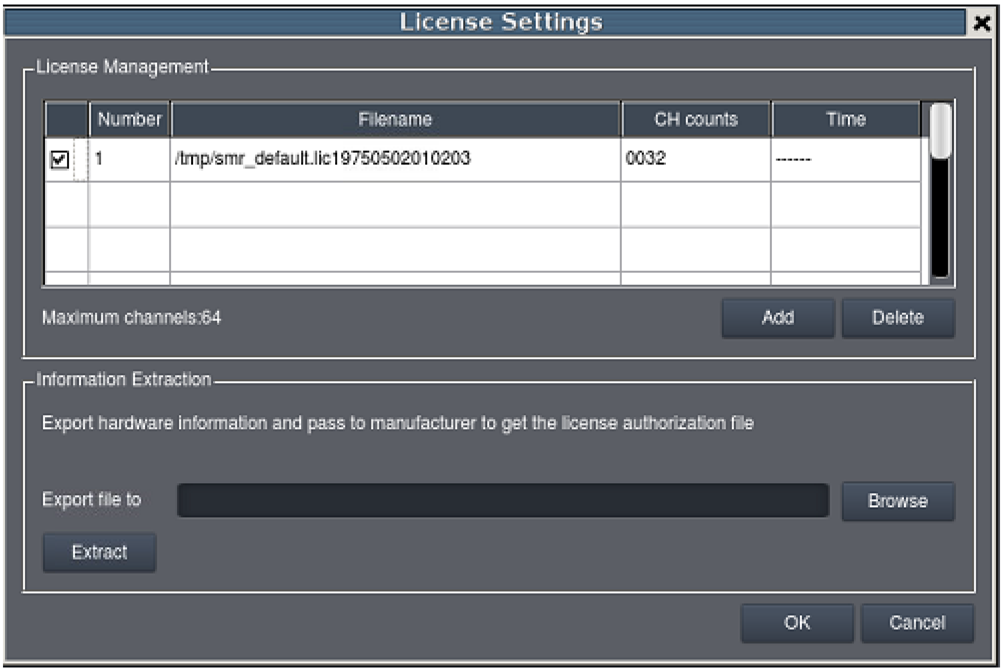
Exporting Parameters

To export parameters into the Server:

1. Select the item that you wish to export by clicking on the item type.
2. Click the **Export** button. A windows explorer dialog will appear.
3. Input a filename and select the export path in the file explorer, and click **Save** to export the file.

11.9.4. License

Extra supported channels can be added by purchasing licenses.



	Number	Filename	CH counts	Time
☑	1	/tmp/smr_default.lic19750502010203	0032	------

Maximum channels:64

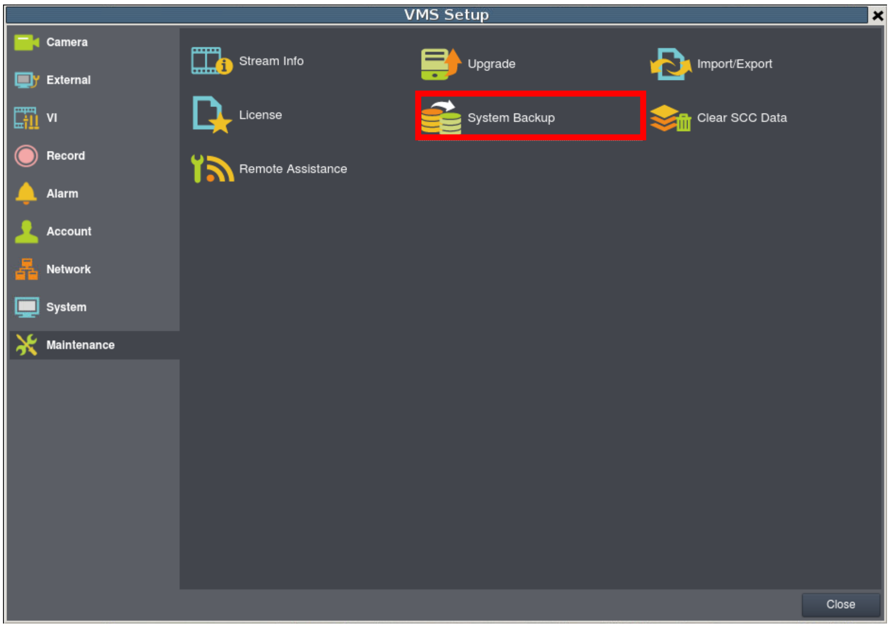
Export hardware information and pass to manufacturer to get the license authorization file

Export file to

1. Click **Browse** under Information Storage Address, and enter a file name for exporting the existing channel information.
2. Click **Extract**. The *.info file will be stored to the selected path or to the default path usually your desktop.
3. Provide the extracted file to your distributors or dealers to acquire the license information. And they will return the license file (“License Key+Channel Number.lis”) for you to add the channels.
4. After receiving the license file, go back to the Local Client Console under setting and click ADD to upload your “xxx.lis” file from the online registration to the VMS add-on channels (License).
5. Check the License Management to make sure if the channels are added successfully. Once your purchased channels are added on, click “OK” to confirm and leave this page.

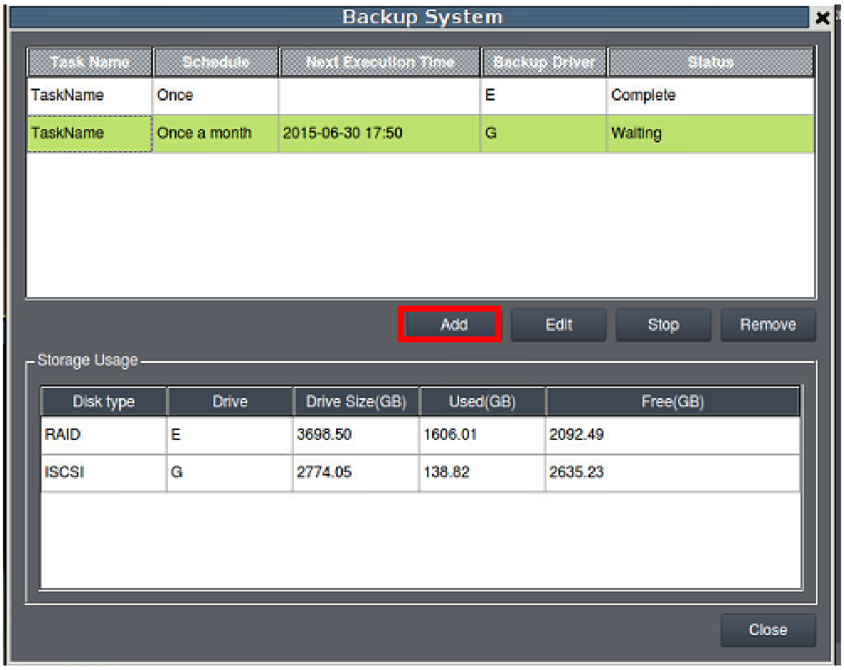
11.9.5. System Backup

The video recordings can be backed up to USB HDD devices and ISCSI. But it is not allowed to use the ones for recording to back up.



Add a Backup Schedule

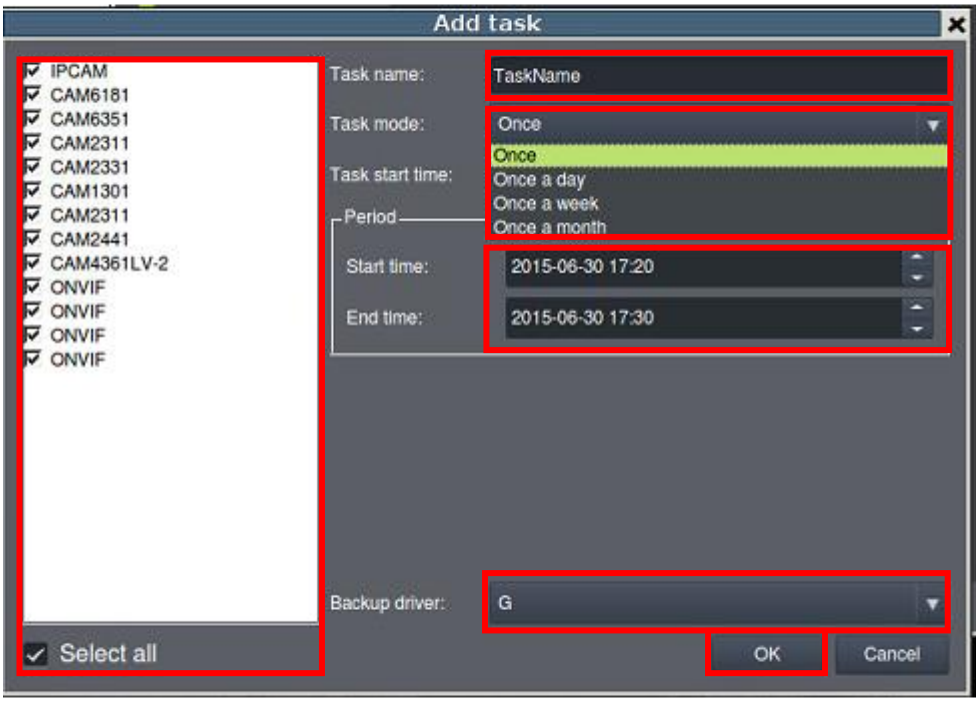
Go to the Maintenance > System Backup. Click **Add** to bring out the Add task window.



Task Name	Schedule	Next Execution Time	Backup Driver	Status
TaskName	Once		E	Complete
TaskName	Once a month	2015-06-30 17:50	G	Waiting

Disk type	Drive	Drive Size(GB)	Used(GB)	Free(GB)
RAID	E	3698.50	1606.01	2092.49
ISCSI	G	2774.05	138.82	2635.23

Add Task Window:



Add task

☑ IPCAM
☑ CAM6181
☑ CAM6351
☑ CAM2311
☑ CAM2331
☑ CAM1301
☑ CAM2311
☑ CAM2441
☑ CAM4361LV-2
☑ ONVIF
☑ ONVIF
☑ ONVIF
☑ ONVIF

☑ Select all

Task name: TaskName

Task mode: Once

Once
Once a day
Once a week
Once a month

Task start time:

Period

Start time: 2015-06-30 17:20

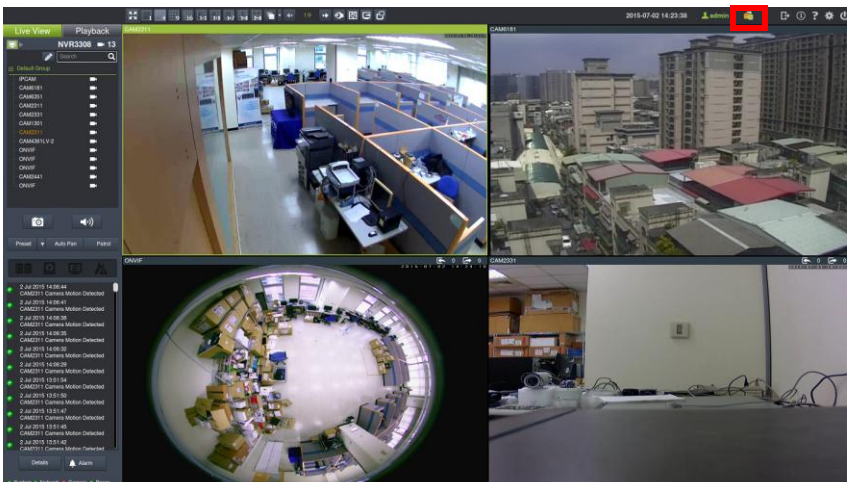
End time: 2015-06-30 17:30

Backup driver: G

OK | Cancel

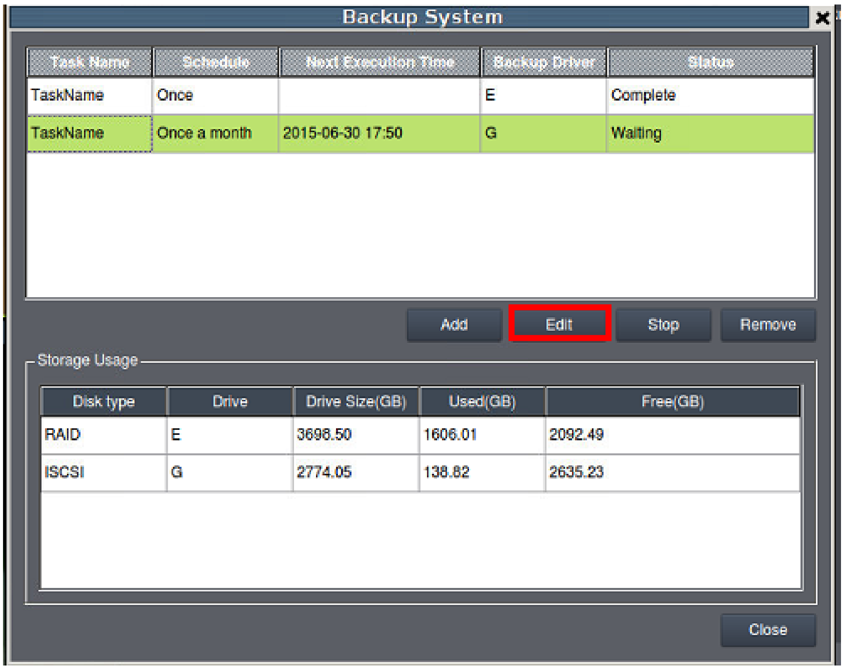
- Select the cameras or check the option **Select all** to set backups.
- Input a Task Name.
- Select a Task Mode: once, once a day, once a week, or once a month.
- Select a start time and an end time.
- Select a backup driver.
- Click **OK** to confirm the setting.

When the system is running the backup tasks, you’ll see an icon on the upper right corner of the liveview page. Click on the icon to go to the backup setup page.



Edit a Backup Schedule

1. Go to the *Maintenance* > *System Backup*. Select the Task you'd like to modify and click **Edit** to bring out the Edit task window.


Backup System

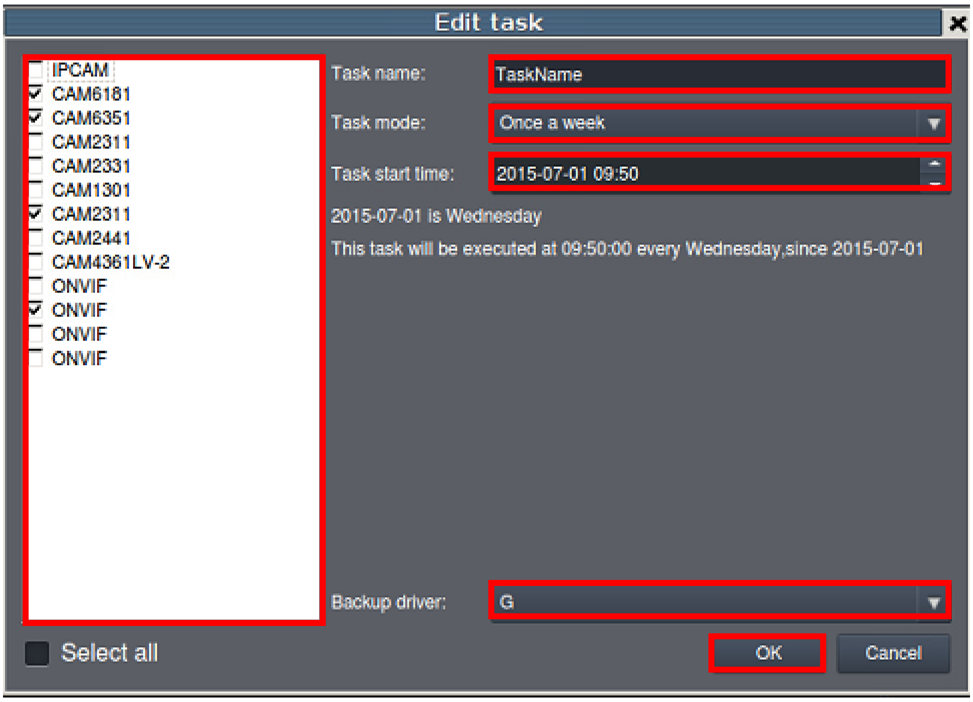
Task Name	Schedule	Next Execution Time	Backup Driver	Status
TaskName	Once		E	Complete
TaskName	Once a month	2015-06-30 17:50	G	Waiting

Storage Usage

Disk type	Drive	Drive Size(GB)	Used(GB)	Free(GB)
RAID	E	3698.50	1606.01	2092.49
ISCSI	G	2774.05	138.82	2635.23

Note: Only tasks in the **waiting** status can be edited. For completed or operating tasks, users can only delete them from the list.

Edit Task Window:


Edit task

- □ IPCAM
- ☑ CAM6181
- ☑ CAM6351
- □ CAM2311
- □ CAM2331
- □ CAM1301
- ☑ CAM2311
- □ CAM2441
- □ CAM4361LV-2
- □ ONVIF
- ☑ ONVIF
- □ ONVIF
- □ ONVIF

Task name: TaskName

Task mode: Once a week

Task start time: 2015-07-01 09:50

2015-07-01 is Wednesday

This task will be executed at 09:50:00 every Wednesday,since 2015-07-01

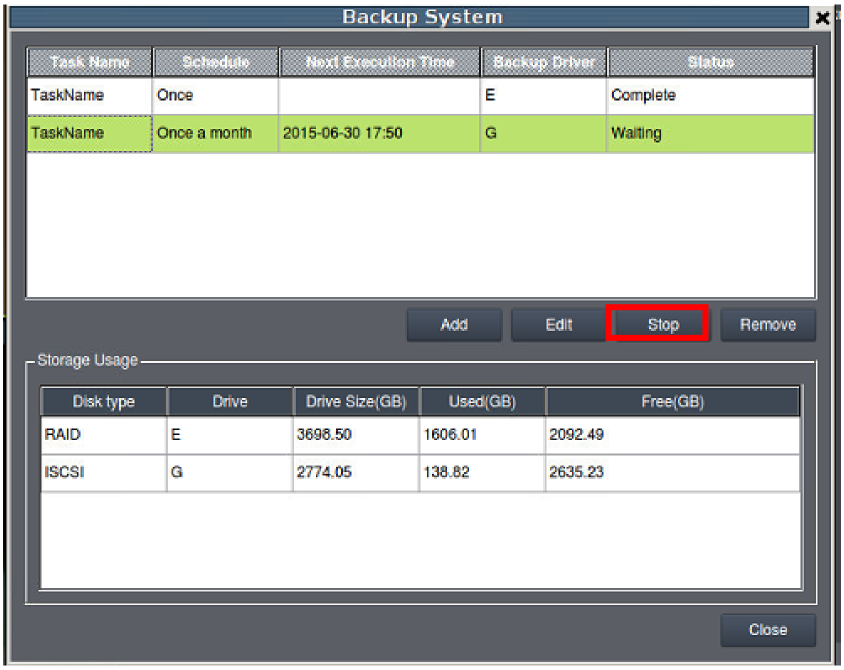
Backup driver: G

□ Select all

- Modify the selected cameras.
- Modify a Task Name.
- Modify the Task Mode: once, once a day, once a week, or once a month.
- Modify the start time.
- Modify the backup driver.
- Click **OK** to confirm the change.

Stop a Backup Schedule

1. Go to the *Maintenance* > *System Backup*. Select the Task you'd like to stop and click **Stop**.



Task Name	Schedule	Next Execution Time	Backup Driver	Status
TaskName	Once		E	Complete
TaskName	Once a month	2015-06-30 17:50	G	Waiting

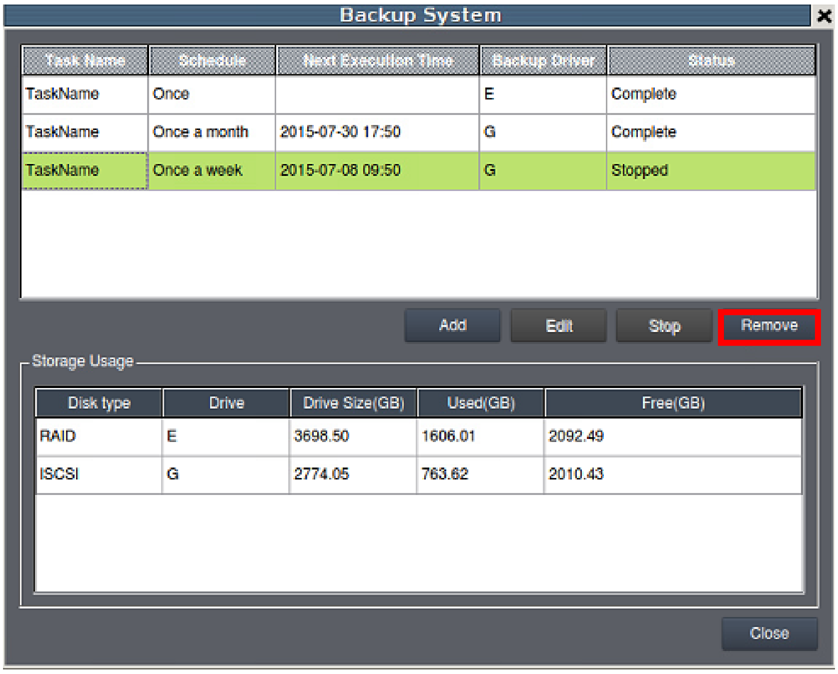
Storage Usage

Disk type	Drive	Drive Size(GB)	Used(GB)	Free(GB)
RAID	E	3698.50	1606.01	2092.49
ISCSI	G	2774.05	138.82	2635.23

Note: Only tasks in the **waiting or running** status can be edited. For completed tasks, users can only delete them from the list. Once the task has been stopped, it cannot be resumed or edited. For tasks in the **stop** status, users can only delete them from the list.

Delete a Backup Schedule

1. Go to the *Maintenance* > *System Backup*. Select the Task you'd like to delete and click **Remove**.

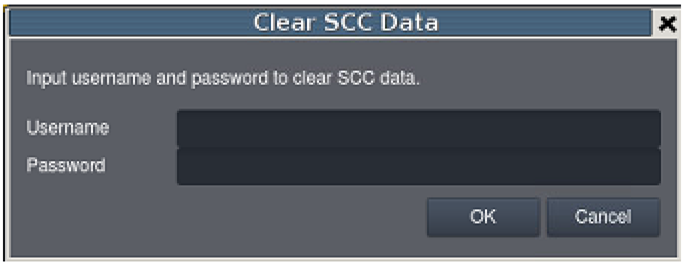


Task Name	Schedule	Next Execution Time	Backup Driver	Status
TaskName	Once		E	Complete
TaskName	Once a month	2015-07-30 17:50	G	Complete
TaskName	Once a week	2015-07-08 09:50	G	Stopped

Disk type	Drive	Drive Size(GB)	Used(GB)	Free(GB)
RAID	E	3698.50	1606.01	2092.49
ISCSI	G	2774.05	763.62	2010.43

11.9.6. Clear SCC Data

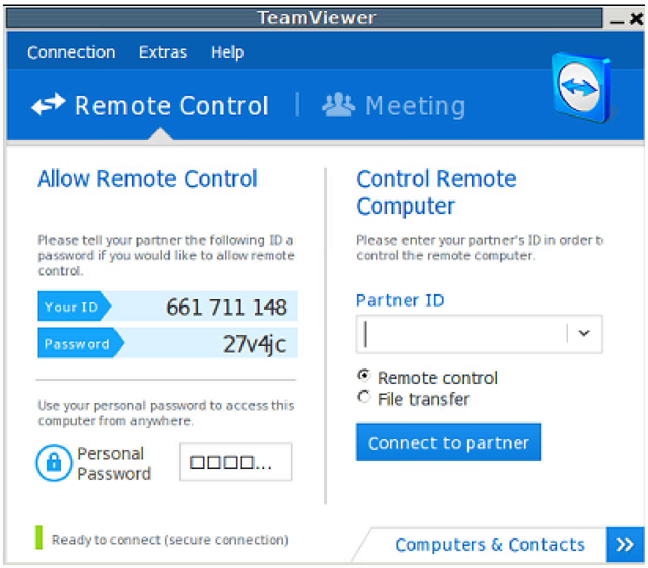
Allows you to clear the SCC /VMS data on the Domain Server.



Input username and password to clear SCC data.

11.9.7. Remote Assistant

This functionality can be used for the technician to have a remote view and controls over your system to determine if there is any problem.



Please tell your partner the following ID a password if you would like to allow remote control.

Your ID 661 711 148

Password 27v4jc

Use your personal password to access this computer from anywhere.

Personal Password □□□□...

Please enter your partner's ID in order t control the remote computer.

● Remote control
○ File transfer

Ready to connect (secure connection)

Chapter 12. Remote Web Client and SPhone Client for Simple Use (Optional)

For remote users, there are 3 methods for viewing.

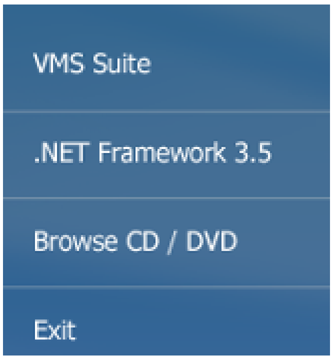
1. Remote Client: install Remote Client on remote PCs for live view and playback.
2. Web Client: use the browser IE (Internet Explorer) and input the IP address of the camera for live view and playback.
3. Mobile Client: install the **Sphone Client** app on iOS or Android mobile devices for basic live viewing.

12.1. Software Installation for Remote Control

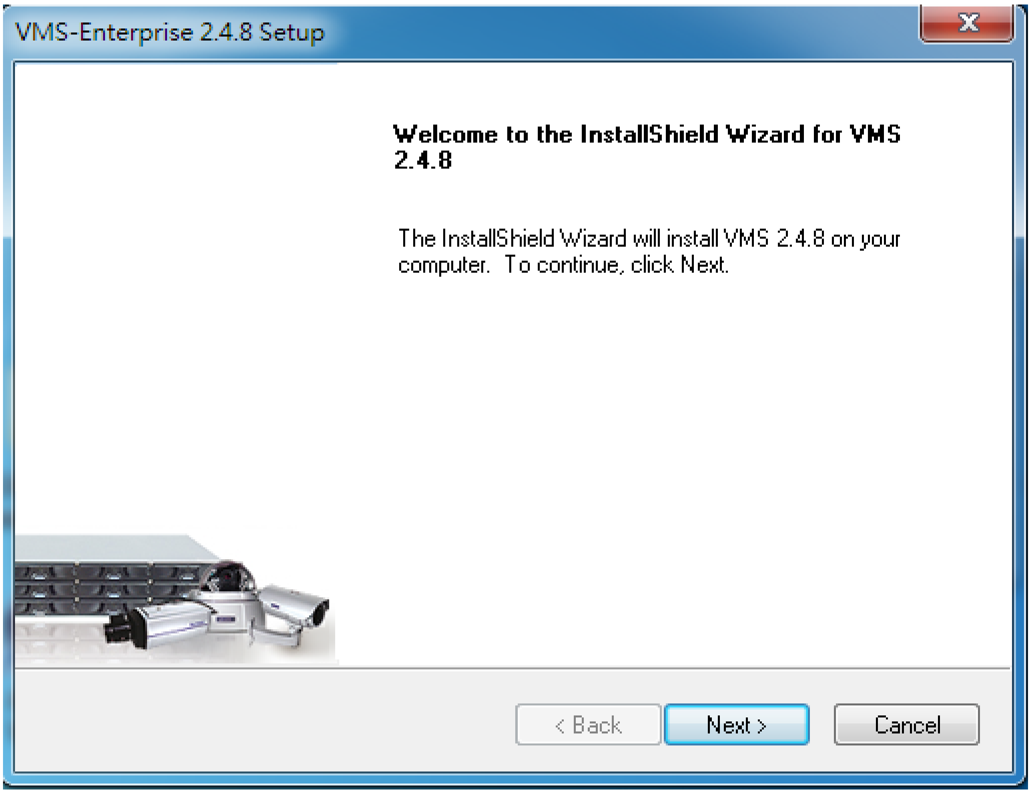
12.1. Installing the VMS

Note: For NVR5000 series, users have to install VMS Client on remote PC(s) when distant live viewing and playback are needed.

1. Insert the VMS/IPCAM CD-ROM. The CD should auto run. If it does not, open the CD manually and double-click **autorun.exe**. The menu below will be displayed.



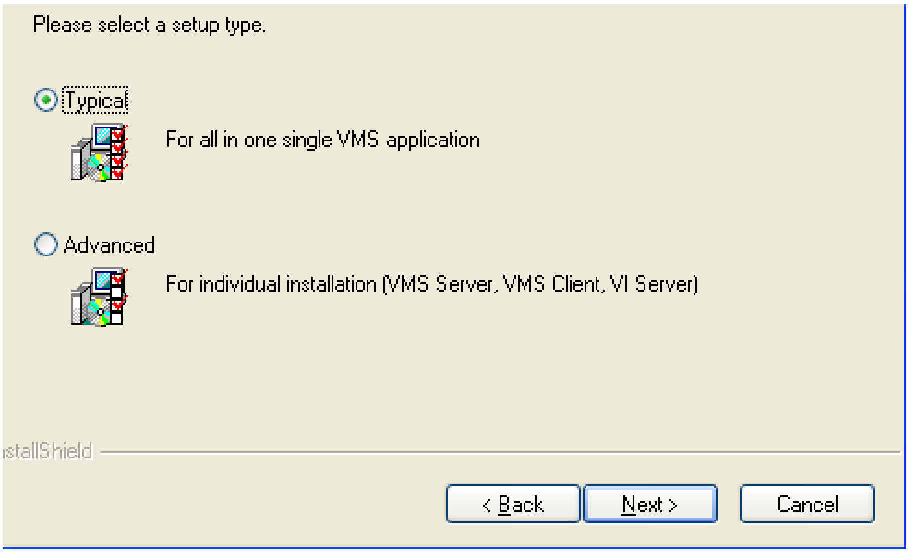
Click **VMS Suite** to start the installation.



Welcome to the InstallShield Wizard for VMS 2.4.8

The InstallShield Wizard will install VMS 2.4.8 on your computer. To continue, click Next.

2. Choose a setup type from *Typical* and *Advanced*. Then Click **Next** when you are satisfied with your selection.



Please select a setup type.

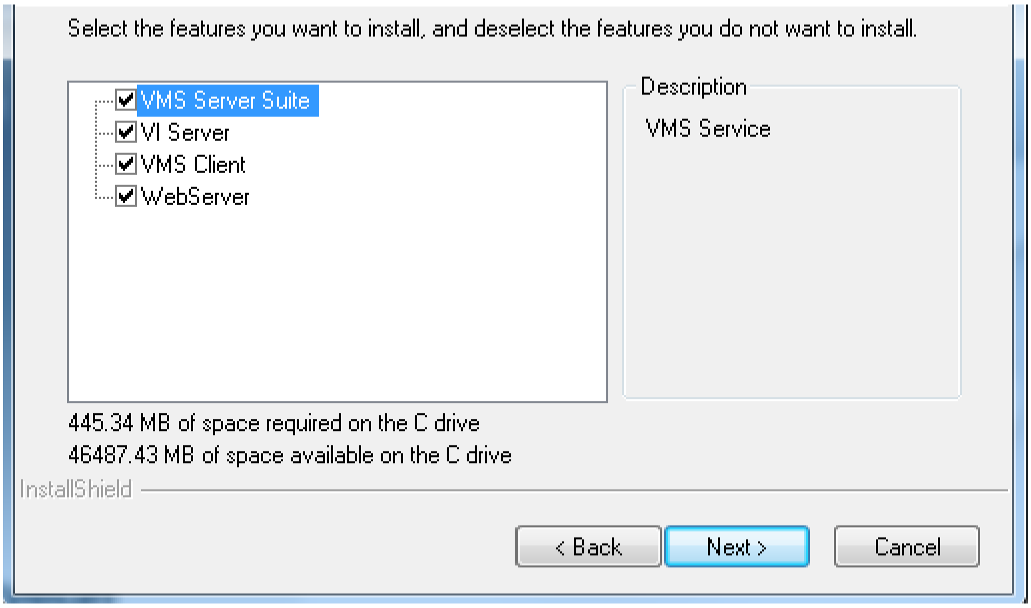
● Typical

For all in one single VMS application

○ Advanced

For individual installation (VMS Server, VMS Client, VI Server)

You may choose to install among the following while *Advanced Setup Type* is selected:



Select the features you want to install, and deselect the features you do not want to install.

☑ VMS Server Suite
☑ VI Server
☑ VMS Client
☑ WebServer

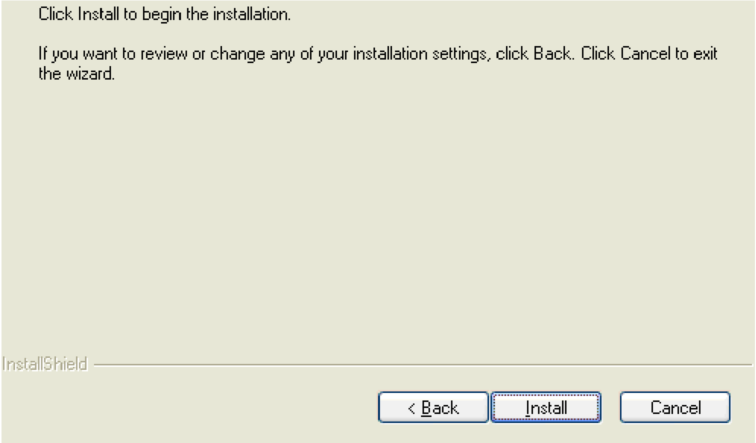
Description

VMS Service

445.34 MB of space required on the C drive
46487.43 MB of space available on the C drive

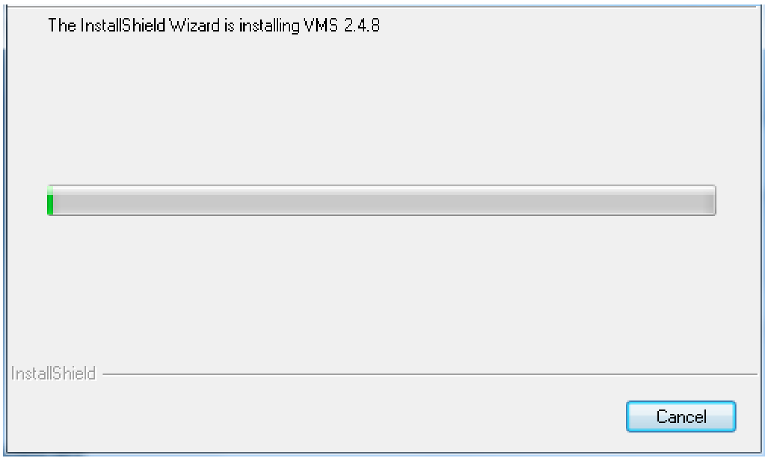
- **VMS Server Suite** – Includes the VMS Server and Local Domain Server, VI Server and VMS Client.
- **VI Server**
- **VMS Client**
- **Web Server**

3. The confirmation screen will display. Click **Install**. A progress bar will display, indicating installation progress.



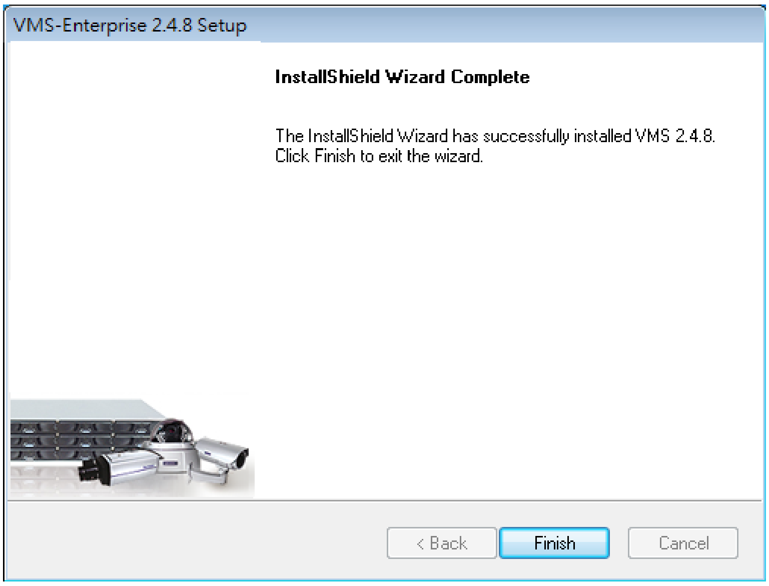
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.



The InstallShield Wizard is installing VMS 2.4.8

4. When installation is finished, an informational screen will display. Click **Finish** to complete installation.

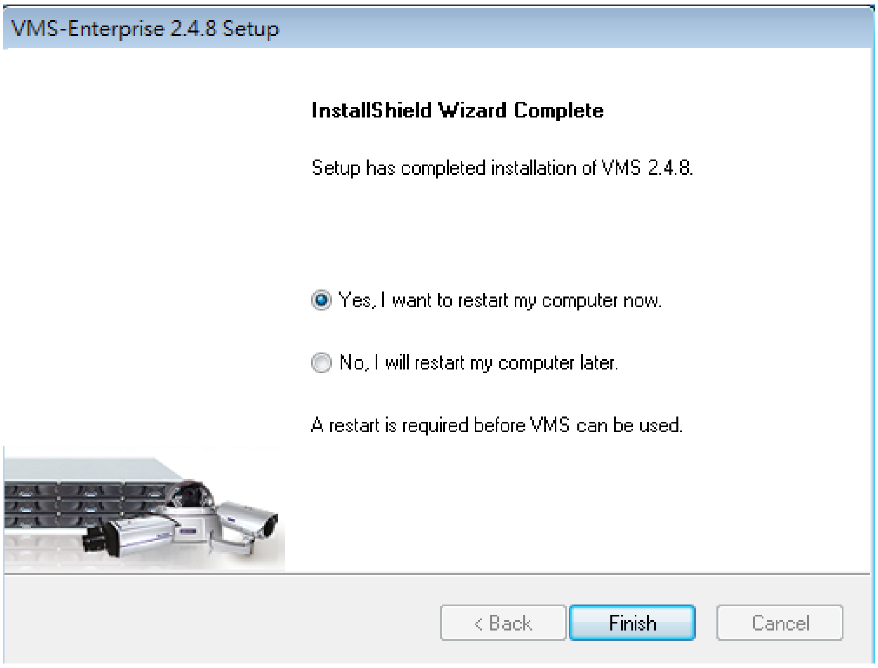


VMS-Enterprise 2.4.8 Setup

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed VMS 2.4.8. Click Finish to exit the wizard.

5. The system will prompt for a restart. A restart is required before the VMS will function correctly. You may choose to immediately automatically restart your computer, or restart your computer later. Clicking **Finish** will apply your choice.



VMS-Enterprise 2.4.8 Setup

InstallShield Wizard Complete

Setup has completed installation of VMS 2.4.8.

● Yes, I want to restart my computer now.

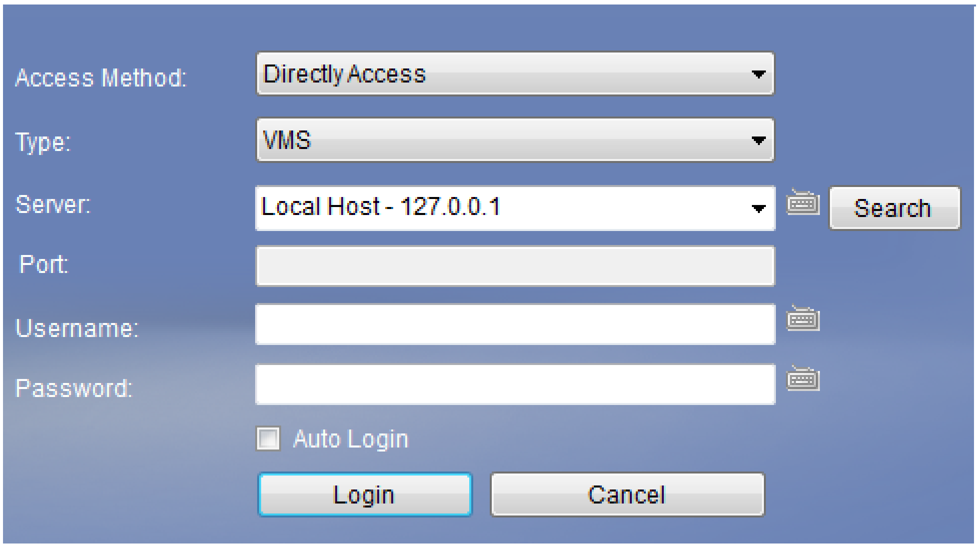
○ No, I will restart my computer later.

A restart is required before VMS can be used.

12.2. Starting the VMS Client

To start the software, click **Programs > VMS Suite > VMS Client** under the Windows **Start** menu.

The software will prompt for the following information:



Access Method: Directly Access

Type: VMS

Server: Local Host - 127.0.0.1

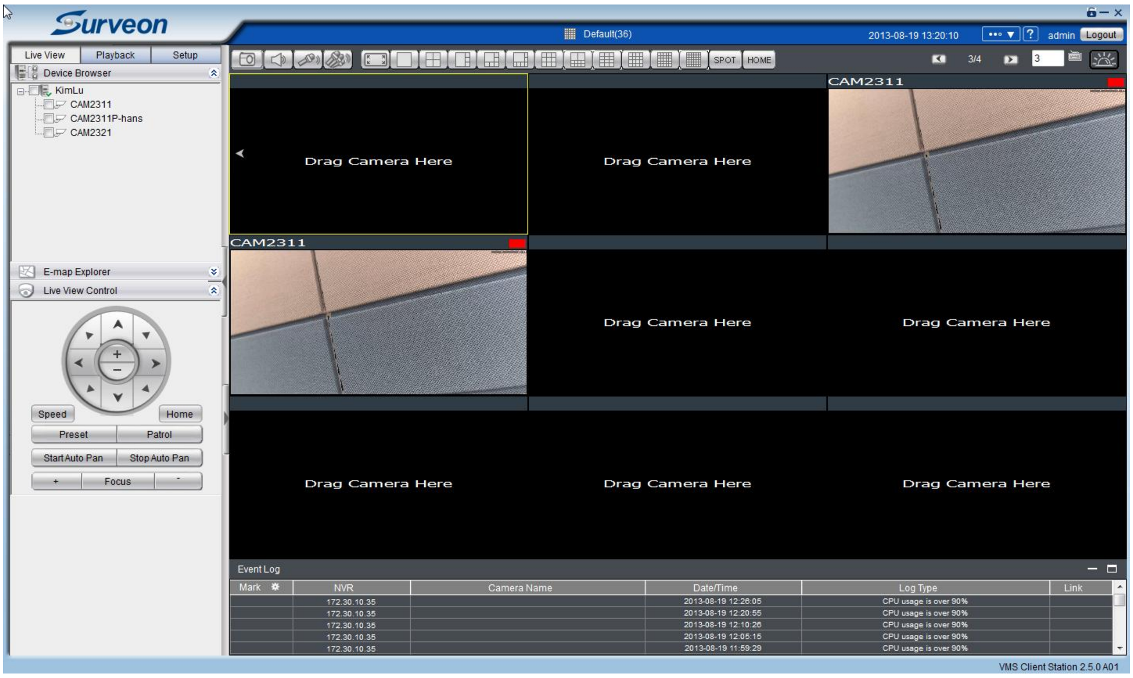
- **Access Method** – Directly Access or Internet Port Forward.
- **Type -** Choose VMS.
- **Server** – The IP address for the VMS/NVR Server. You can click **Search** button to obtain it. For users of port forwarding, it should be the IP address of the router.
- **Port -** The Login Port for port forwarding - 9050. It should be set under ***Server* > *Other Tasks* > *Port Mapping*** after the first login.

Note: (1) Please refer to *Port Forwarding Section* for more details. (2) SCC does not support port forwarding functionalities.

- **Username** – The username for the domain, **which is always *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**

Click **Login** after the password (and port number) is entered.

After logged in, you’ll see the following images.



Mark	NVR	Camera Name	Date/Time	Log Type	Link
	172.30.10.35		2013-08-19 12:26:05	CPU usage is over 90%	
	172.30.10.35		2013-08-19 12:20:55	CPU usage is over 90%	
	172.30.10.35		2013-08-19 12:10:26	CPU usage is over 90%	
	172.30.10.35		2013-08-19 12:05:15	CPU usage is over 90%	
	172.30.10.35		2013-08-19 11:59:29	CPU usage is over 90%	

For VMS Remote Client configurations, please refer to the VMS User Manual.

12.2.1. Logging out

The Client can be logged out of all the Servers configured on the system by pressing the **Logout** button on the upper right hand corner in the GUI. Logging out of individual servers can be achieved by double clicking the server entry and clicking the **Yes** button on the confirmation screen.

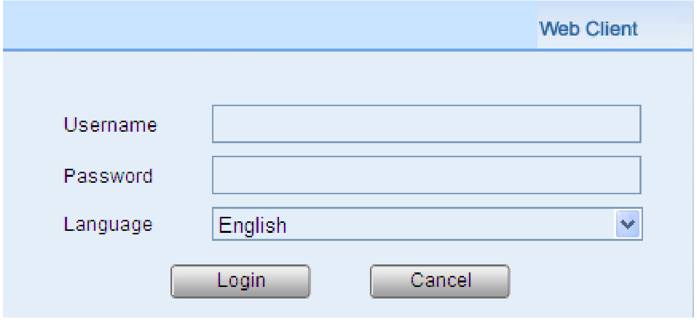
Note: (1) If the system becomes unresponsive, users can force shutdown the system (press and hold the power until the system shuts down). This should only be done when the system is unresponsive!

12.3. Starting the Web Client

Launch Microsoft Internet Explorer 7.0 (or above) and enter your **VMS Server IP address + "/webclient"** in your web browser's URL location, e.g. http://172.18.6.9/webclient to download the Web Client application.

Note: Please check the web server settings in the VMS Setup first.

After the Web Client installation is done, a login window will pop up.



- **Username** – The username for the domain. **Default username is *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**
- **Language** -Options for the interface languages.

Click **Login** after the username and password are entered.

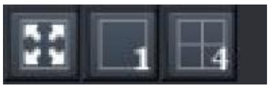
After logging in, the live view page will be displayed on the web browser.

12.3.1. Checking the Software Version

Users can see the software version at the lower left corner of the window after logging in.

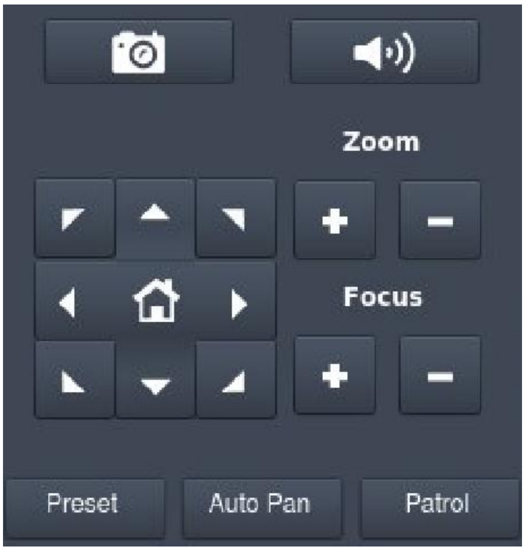
12.3.2. Use of 1x/4x views

Users have the option of viewing up to 4 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.

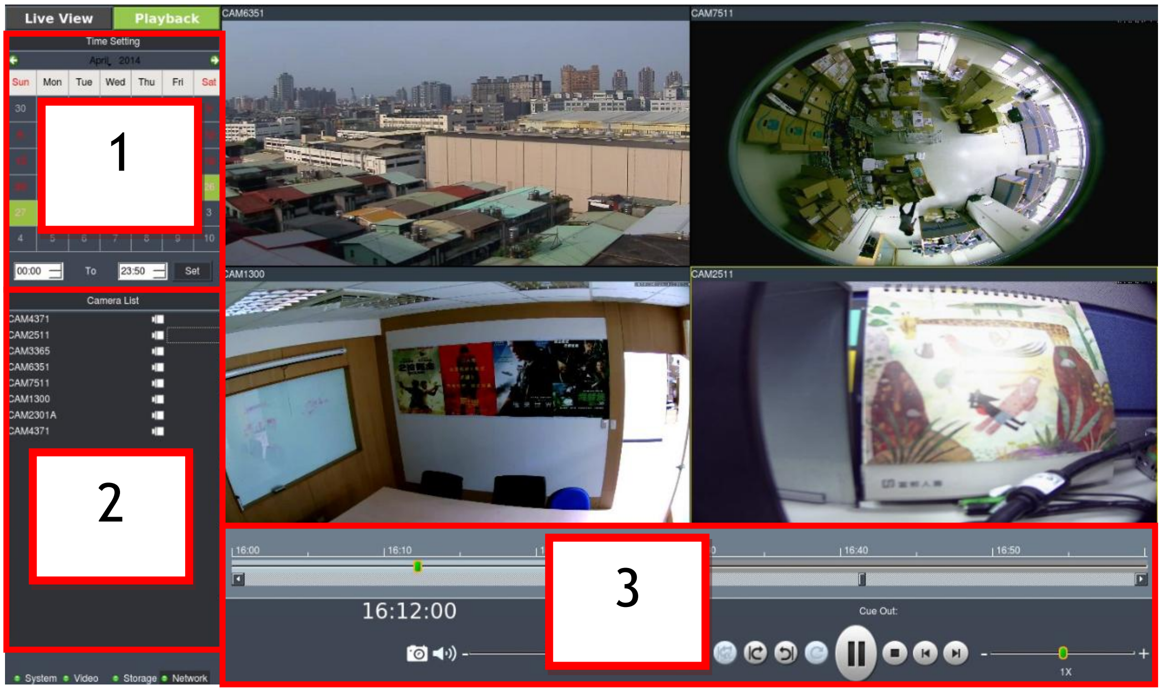


12.3.3. PTZ Control

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the Web Client. These controls can be found in the *PTZ Control* window within the live view screen.



12.3.4. Playback Settings



Users can select the (1) time and (2) camera, and then use the (3) time line and playback control panel to do the playback.

Note: For more details of PTZ Control and Playback Control, please refer to PTZ Control and Playback sections in this chapter.

12.4. Installing and Starting the SPhone Client on iOS Devices

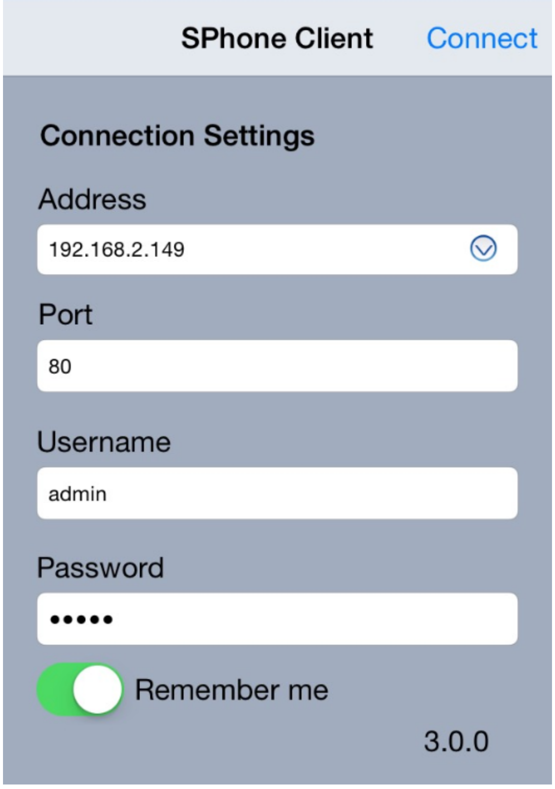
12.4.1. Installing the SPhone Client (Optional)

Download the SPhone Client from App Store on the iPhone desktop.

12.4.2. Starting the SPhone Client

Note: Please check the web server settings in the VMS Setup first.

After the SPhone Client installation is done, a login window will pop up.



Connection Settings

Address: 192.168.2.149

Port: 80

Username: admin

Password: •••••

Remember me

3.0.0

- **Address**: The IP address for the VMS/SMR Server.
- **Port:** The login port for SPhone Client. **Default port number is *80*.**

Note: The port number should be the same with the web server port.

- **Username** – The username for the domain. **Default username is *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**

Click **Connect** on the upper right corner after the port, username and password are entered.

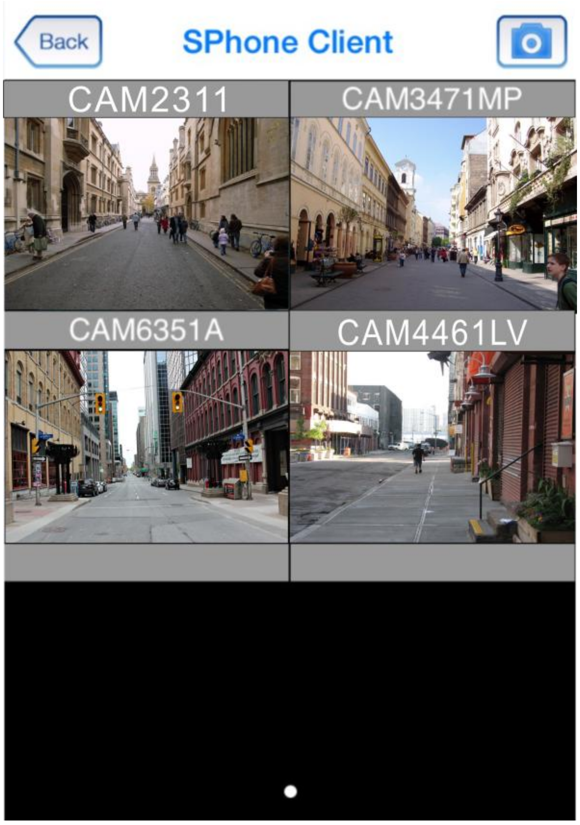
12.4.3. Checking the Software Version

Users can see the software version at the lower right corner of the window after logging in.

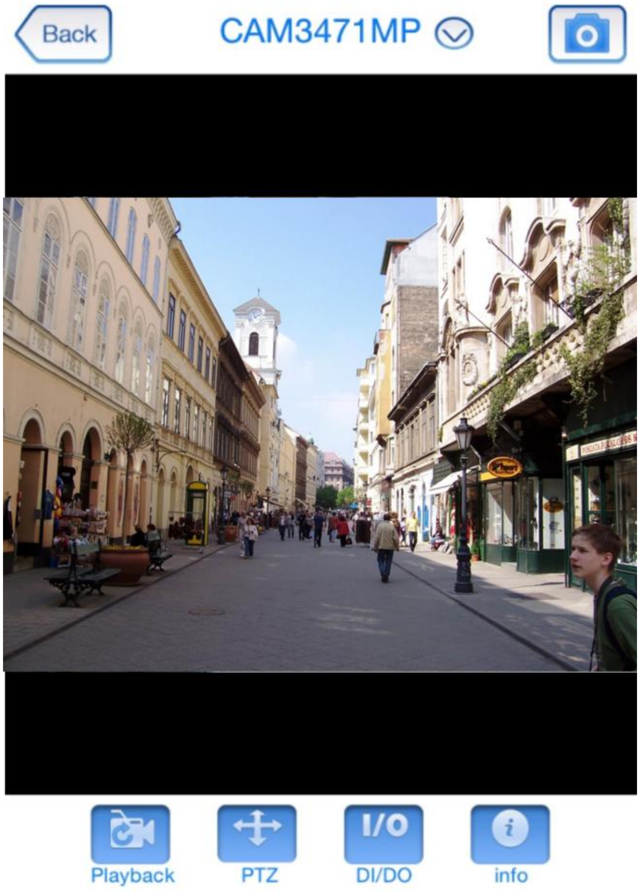
12.4.4. Functionalities on the SPhone Client

Live View

After logging in, you will see the Live View images. The default is 6 channels per page.



You can click on any channel you'd like to see or manage to have a single view on your device.



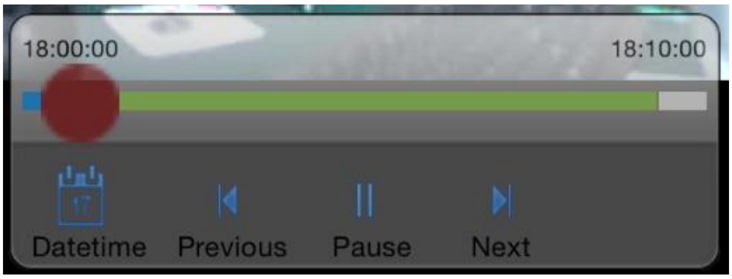
Icon Descriptions

Icon	Function
Back	Use the Back icon to go back to the previous page.
📷	Use the snapshot icon to take a snapshot of the current view.
⌄	After tapping this icon, there'll be a drop-down list for you to select a camera to view or manage.
Playback	Use the playback icon to view the recorded video from the current camera.
PTZ	Use the PTZ icon to perform a Pan, tilt, zoom functionality.
Preset	After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points. Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.
I/O DI/DO	Tap the icon to see the camera digital input/output status.
i info	Tap the icon to see a detailed information

Playback

After tapping on the Playback icon , Playback you'll see the image below.

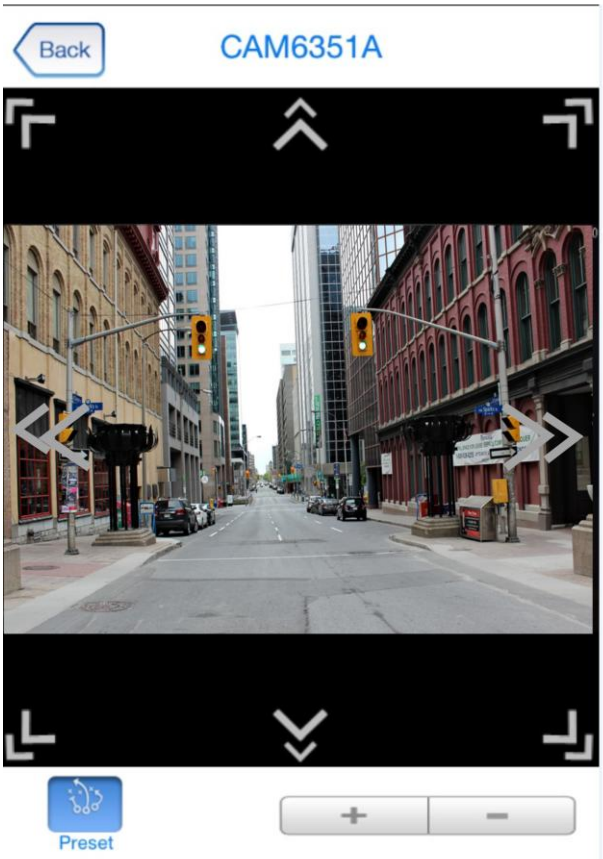
Use the icons on this page to set the date/time to search for the specified videos and use the Previous/Next, Play/Pause icons to view the recorded videos.



PTZ/Preset

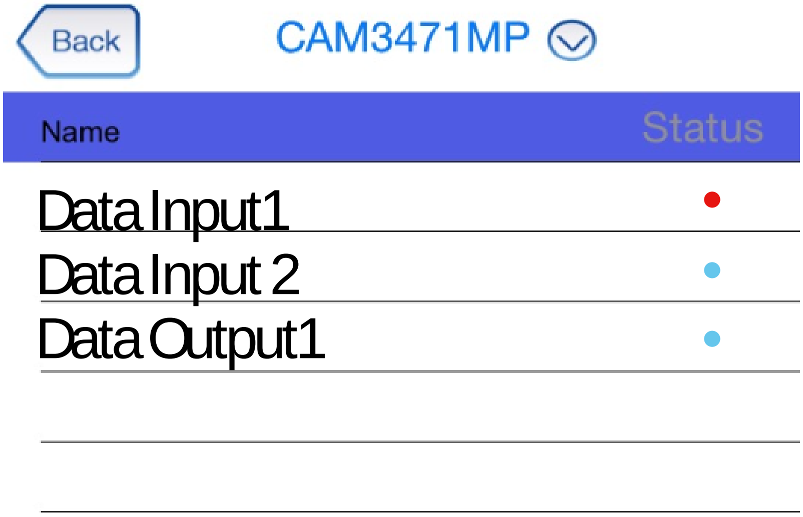
After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points.

Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.



DI/DO

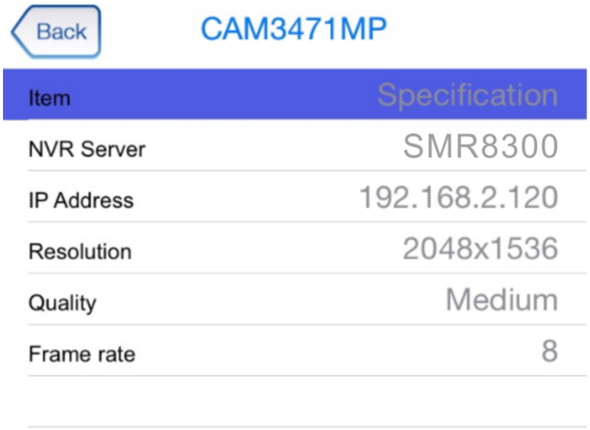
Tap this icon to see the camera digital input/output status.



Name	Status
Data Input1	🔴
Data Input 2	🔵
Data Output1	🔵

Info

The icon ⓘ info can be used to check the detailed information of each camera as follows.



Item	Specification
NVR Server	SMR8300
IP Address	192.168.2.120
Resolution	2048x1536
Quality	Medium
Frame rate	8

- **NVR Server:** The VMS/SMR Server name
- **IP Address:** The IP address for the VMS/SMR Server
- **Resolution:** The video resolution of the camera
- **Quality:** The video quality of the camera
- **Frame Rate :** The frame rate of the camera

12.5. Installing and Starting the SPhone Client on Android Devices

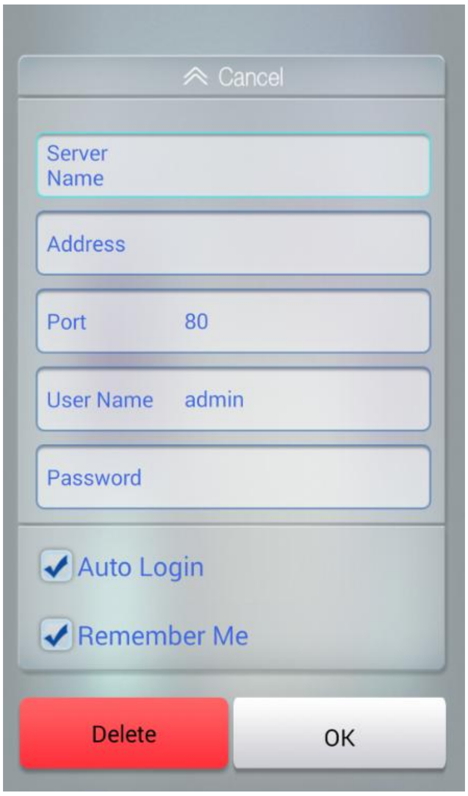
12.5.1. Installing the SPhone Client (Optional)

Download the SPhone Client from App Store on the Android phone desktop.

12.5.2. Starting the SPhone Client

Note: Please check the web server settings in the VMS Setup first.

After the SPhone Client installation is done, a login window will pop up.



Server Name

Address

Port 80

User Name admin

Password

☑ Auto Login

☑ Remember Me

- **Server Name:** The VMS/SMR Server Name
- **Address**: The IP address for the VMS/SMR Server.
- **Port:** The login port for SPhone Client. **Default port number is *80*.**

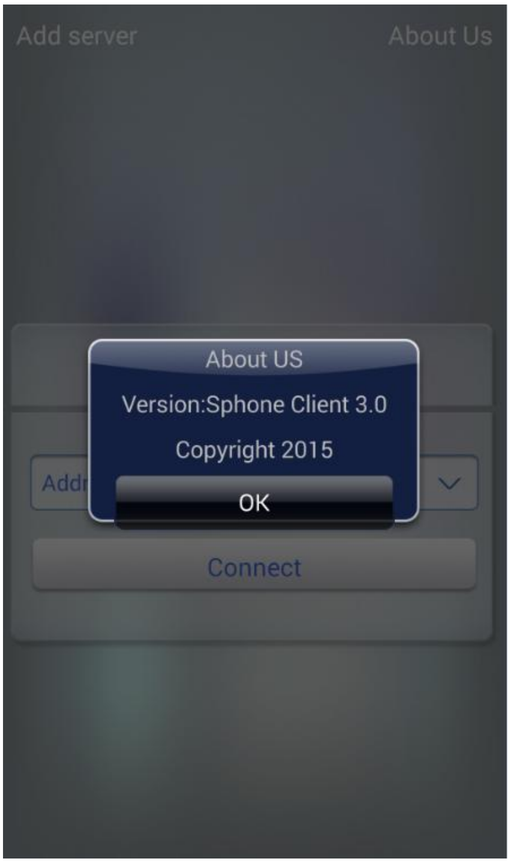
Note: The port number should be the same with the web server port.

- **Username** – The username for the domain. **Default username is *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**

Click **OK** icon after the port, username and password are entered.

12.5.3. Checking the Software Version

Users can see the software version. Tap on the About Us on the upper right corner of the window after logging in.



About US

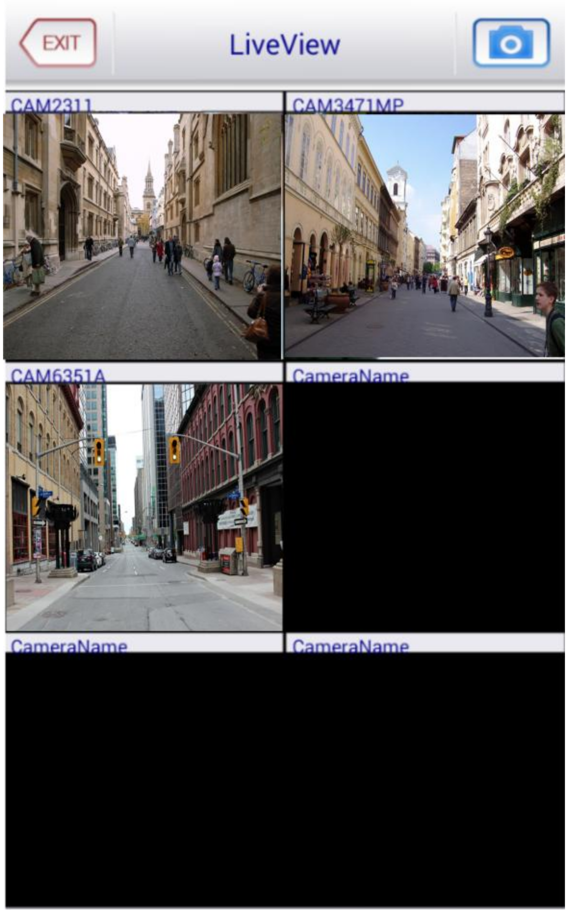
Version:Sphone Client 3.0

Copyright 2015

12.5.4. Functionalities on the SPhone Client

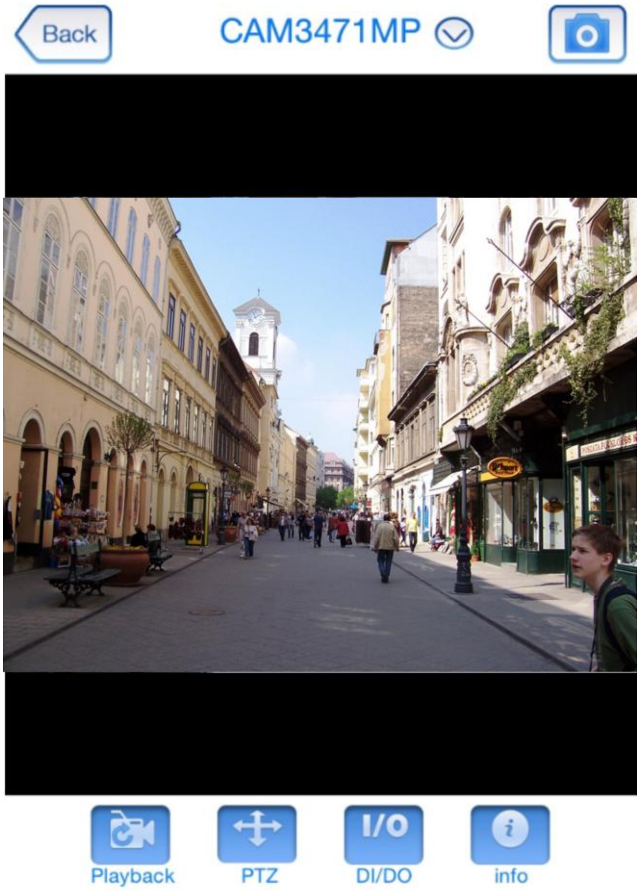
Live View

After logging in, you will see the Live View images. The default is 6 channels per page.



At most 6-channel live view can be displayed in the same page.

You can click on any channel you'd like to see or manage to have a single view on your device.



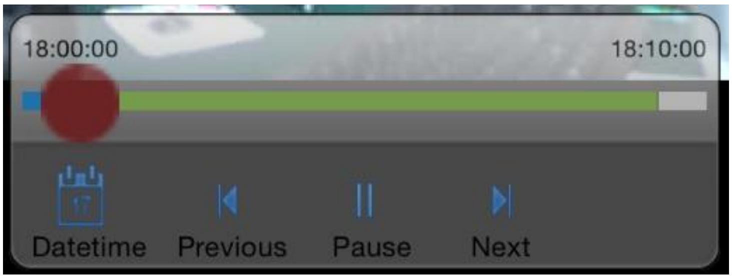
Icon Descriptions

Icon	Function
EXIT	Use the Back icon to leave this page.
📷	Use the snapshot icon to take a snapshot of the current view.
⌄	After tapping this icon, there’ll be a drop-down list for you to select a camera to view or manage.
Playback	Use the playback icon to view the recorded video from the current camera.
✥ PTZ	Use the PTZ icon to perform a Pan, tilt, zoom functionality.
Preset	After tapping the PTZ icon, you’ll also see a Preset icon. Use the Preset icon to monitor the set preset points. Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.
I/O DI/DO	Tap the icon to see the camera digital input/output status.
i info	Tap the icon to see a detailed information

Playback

After tapping on the Playback icon , Playback you'll see the image below.

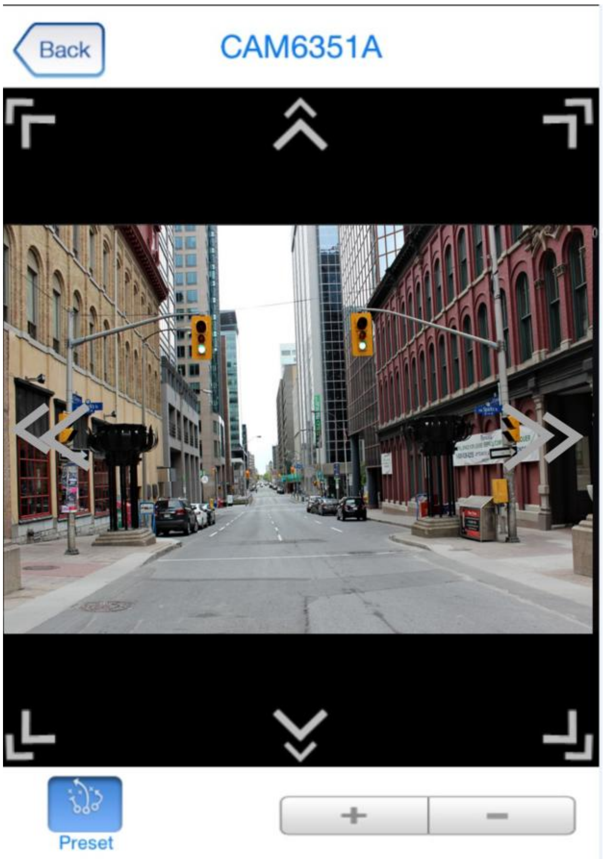
Use the icons on this page to set the date/time to search for the specified videos and use the Previous/Next, Play/Pause icons to view the recorded videos.



PTZ/Preset

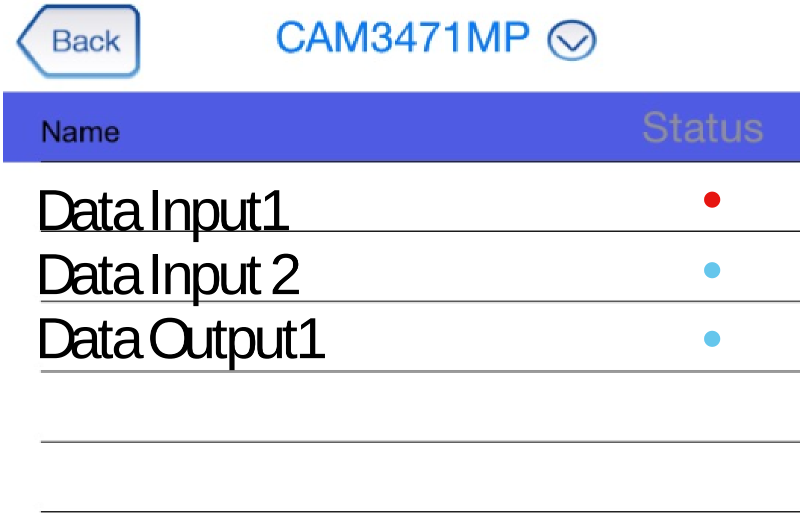
After tapping the PTZ icon, you'll also see a Preset icon. Use the Preset icon to monitor the set preset points.

Presets should be made beforehand. Refer to the Chapter 8 for PTZ Preset settings.



DI/DO

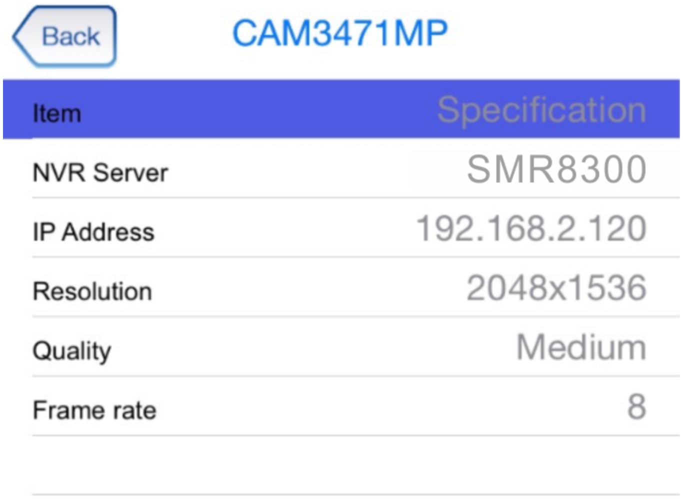
Tap this icon to see the camera digital input/output status.



Name	Status
Data Input1	🔴
Data Input 2	🔵
Data Output1	🔵

Info

The icon ⓘ info can be used to check the detailed information of each camera as follows.



Item	Specification
NVR Server	SMR8300
IP Address	192.168.2.120
Resolution	2048x1536
Quality	Medium
Frame rate	8

- **NVR Server:** The VMS/SMR Server name
- **IP Address:** The IP address for the VMS/SMR Server
- **Resolution:** The video resolution of the camera
- **Quality:** The video quality of the camera
- **Frame Rate :** The frame rate of the camera

Chapter 13. SurveOne (Optional)

SurveOne is a smart web-based system health check tool. The health of the overall systems, including NVRs, cameras, and storage is constantly monitored to achieve the system stability. SurveOne can also simplify setup allowing users to copy the hardware configurations and apply them to other devices to save time and efforts. For easy maintenance, the 3 level-classified real-time event logs, critical errors, errors and warnings, help users to take action efficiently, and thus mitigate risks and reduce losses.

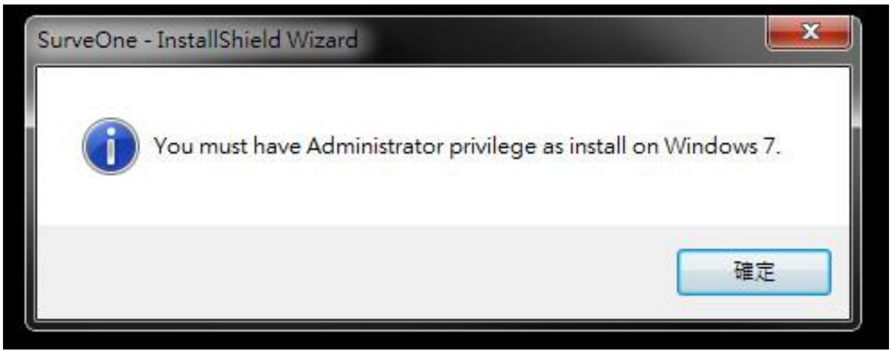
13.1. Installation

Once you have the software file, click to install and follow the installation steps.

Welcome to SurveOne Installation

Please wait.....SurveOne installation is starting

The system will warn you that you'll need to have the administrator privilege as install on Window 7.

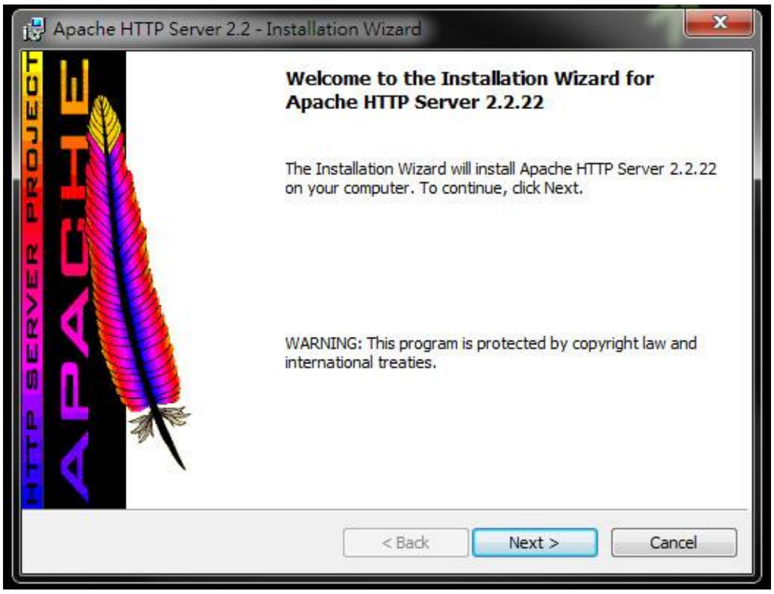


SurveOne - InstallShield Wizard

You must have Administrator privilege as install on Windows 7.

After confirmation, you can start the installation.

1. The installation wizard started. Click **Next**.



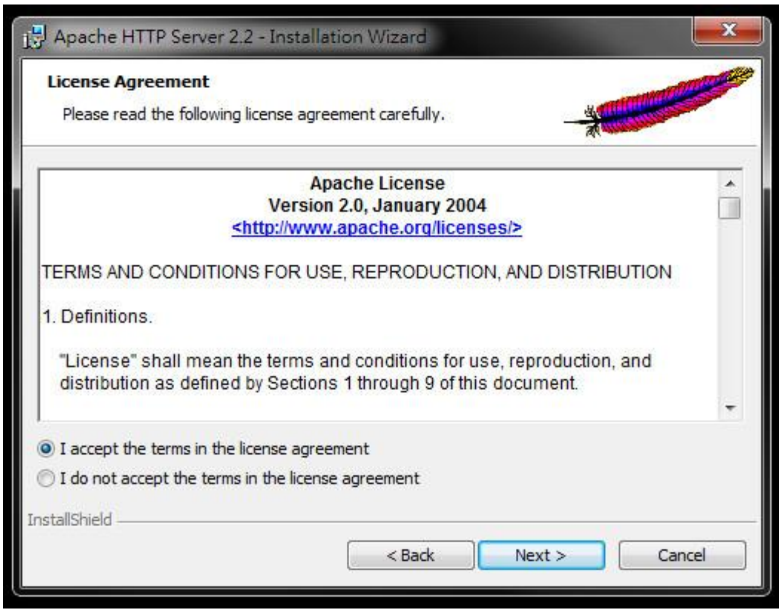
Apache HTTP Server 2.2 - Installation Wizard

Welcome to the Installation Wizard for Apache HTTP Server 2.2.22

The Installation Wizard will install Apache HTTP Server 2.2.22 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. Accept the terms in the license agreement and click **Next**.



Apache HTTP Server 2.2 - Installation Wizard

License Agreement

Please read the following license agreement carefully.

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

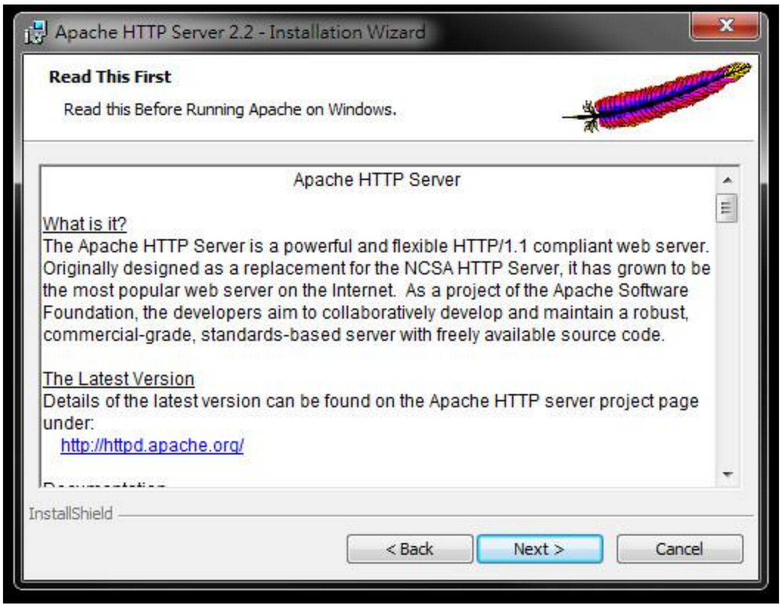
1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

3. Accept and click **Next**.



Apache HTTP Server 2.2 - Installation Wizard

Read This First

Read this Before Running Apache on Windows.

Apache HTTP Server

What is it?

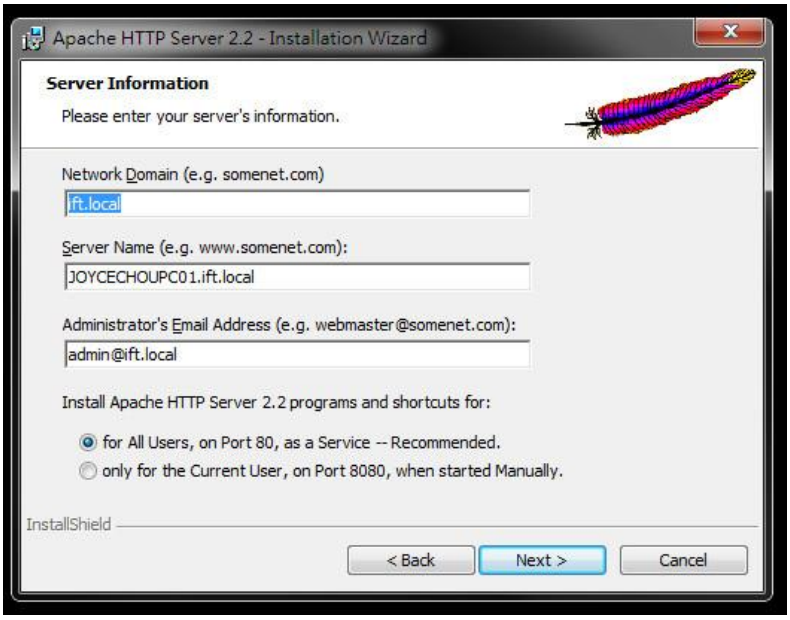
The Apache HTTP Server is a powerful and flexible HTTP/1.1 compliant web server. Originally designed as a replacement for the NCSA HTTP Server, it has grown to be the most popular web server on the Internet. As a project of the Apache Software Foundation, the developers aim to collaboratively develop and maintain a robust, commercial-grade, standards-based server with freely available source code.

The Latest Version

Details of the latest version can be found on the Apache HTTP server project page under:

http://httpd.apache.org/

4. See if there’s any information you’d like to change, if not click **Next**.



Apache HTTP Server 2.2 - Installation Wizard

Server Information

Please enter your server's information.

Network Domain (e.g. somenet.com): ift.local

Server Name (e.g. www.somenet.com): JOYCECHOUPC01.ift.local

Administrator's Email Address (e.g. webmaster@somenet.com): admin@ift.local

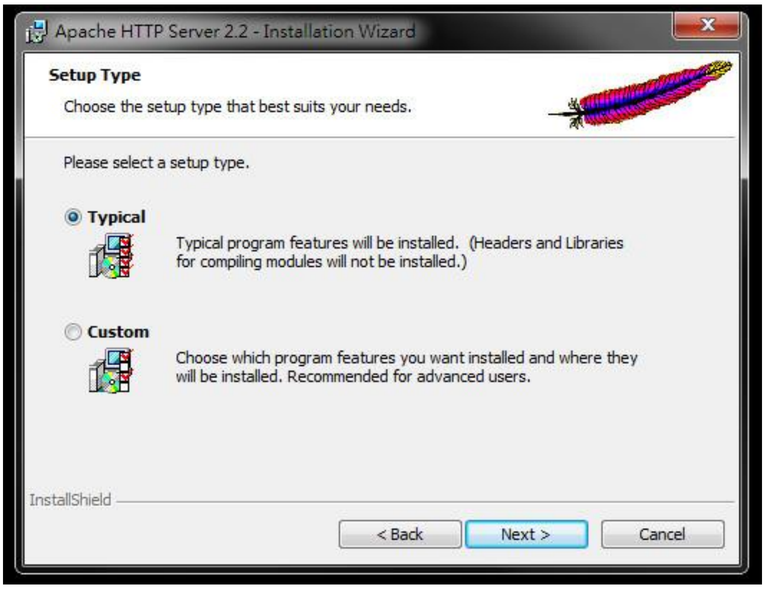
Install Apache HTTP Server 2.2 programs and shortcuts for:

● for All Users, on Port 80, as a Service -- Recommended.

○ only for the Current User, on Port 8080, when started Manually.

5. Select the setup type, typical or custom and click **Next**.

If you are not sure which one to select, it is recommended to select Typical.



Apache HTTP Server 2.2 - Installation Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

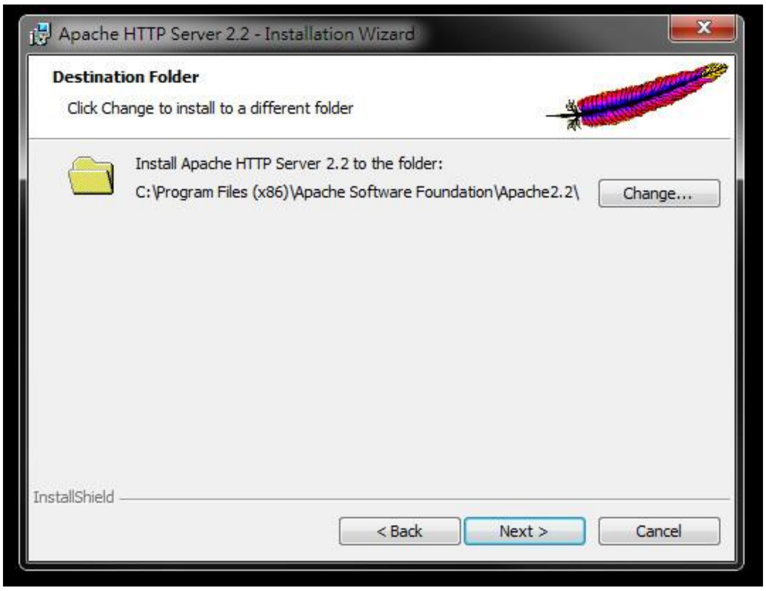
● **Typical**

Typical program features will be installed. (Headers and Libraries for compiling modules will not be installed.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

6. See if you'd like to change the destination folder, click **Change**, if not click **Next**.



Apache HTTP Server 2.2 - Installation Wizard

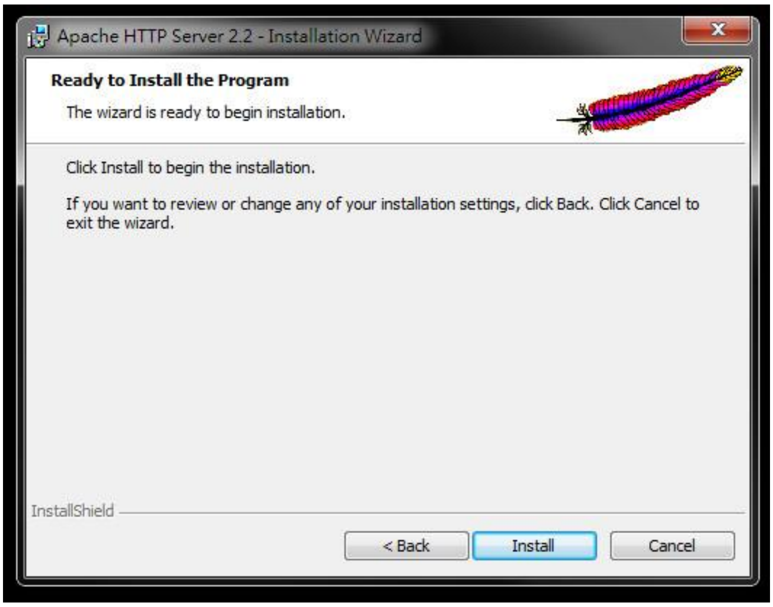
Destination Folder

Click Change to install to a different folder

Install Apache HTTP Server 2.2 to the folder:

C:\Program Files (x86)\Apache Software Foundation\Apache2.2\

7. Click **Install** to start the installation.



Apache HTTP Server 2.2 - Installation Wizard

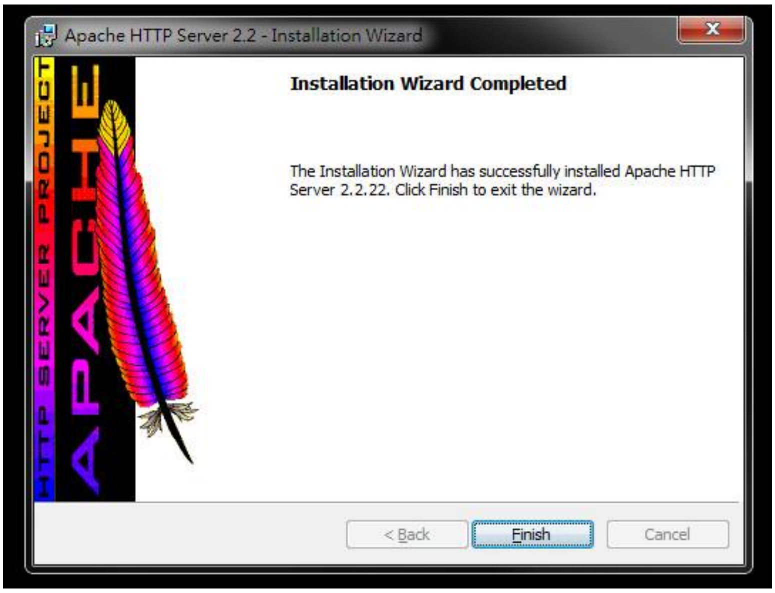
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

8. When the installation wizard completed, click **Finish**.

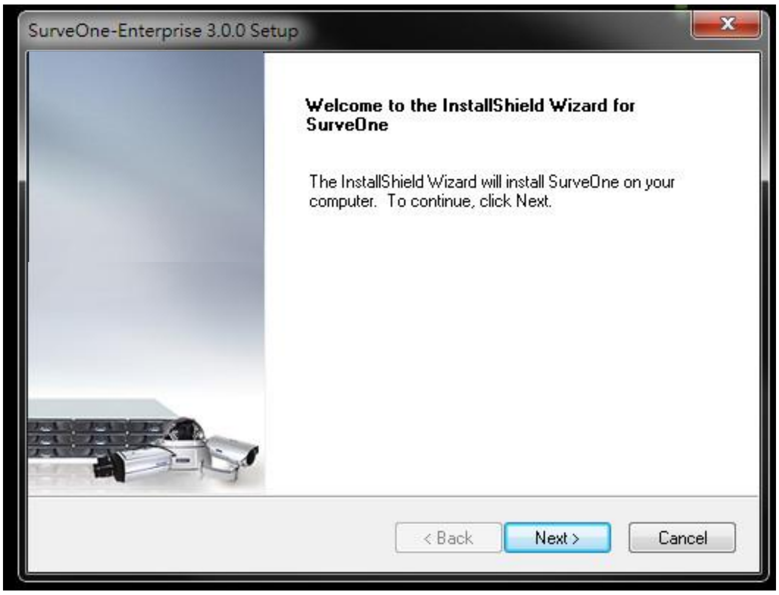


Apache HTTP Server 2.2 - Installation Wizard

Installation Wizard Completed

The Installation Wizard has successfully installed Apache HTTP Server 2.2.22. Click Finish to exit the wizard.

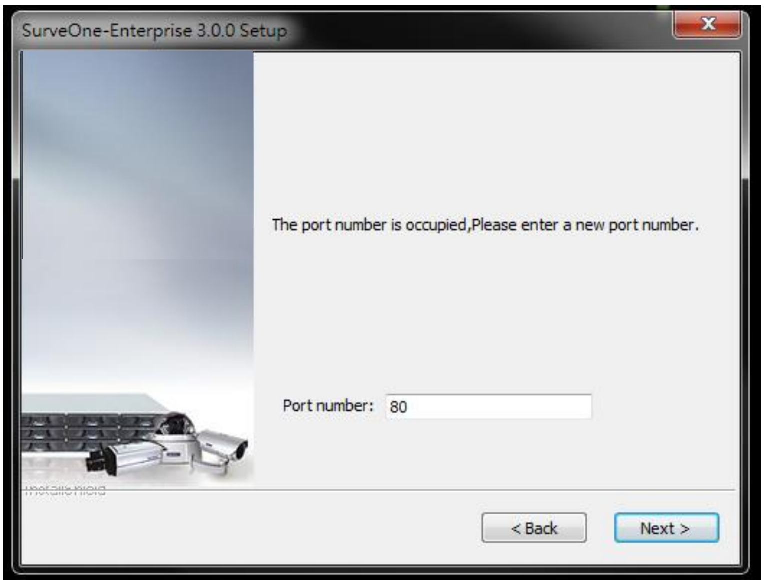
9. Then the SurveOne Installation Wizard will start. Click **Next**.



Welcome to the InstallShield Wizard for SurveOne

The InstallShield Wizard will install SurveOne on your computer. To continue, click Next.

10. Input the port which is not occupied and click **Next**.

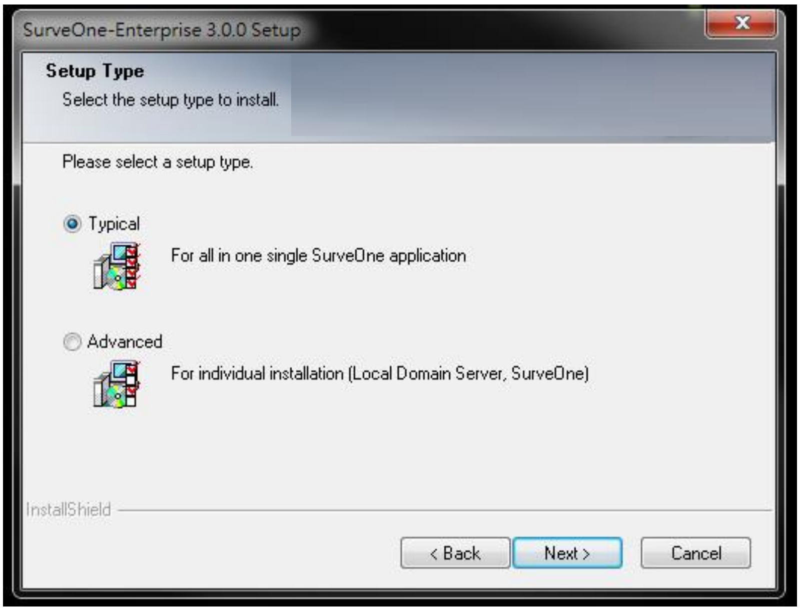


The port number is occupied,Please enter a new port number.

Port number: 80

11. Select the setup type, Typical or Advanced and then click **Next**.

If you are not sure which one to select, it is recommended to select Typical.



SurveOne-Enterprise 3.0.0 Setup

Setup Type

Select the setup type to install.

Please select a setup type.

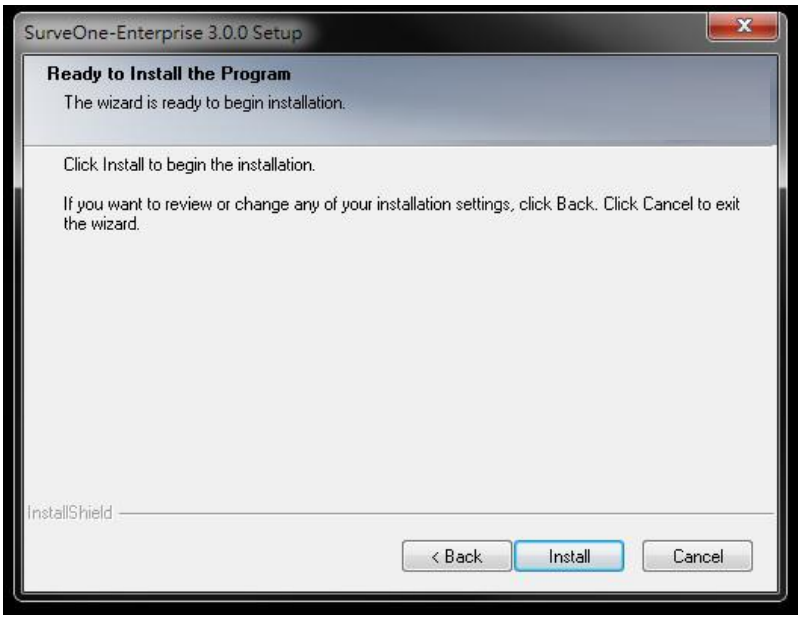
● Typical

For all in one single SurveOne application

○ Advanced

For individual installation (Local Domain Server, SurveOne)

12. Start to install the SurveOne.



SurveOne-Enterprise 3.0.0 Setup

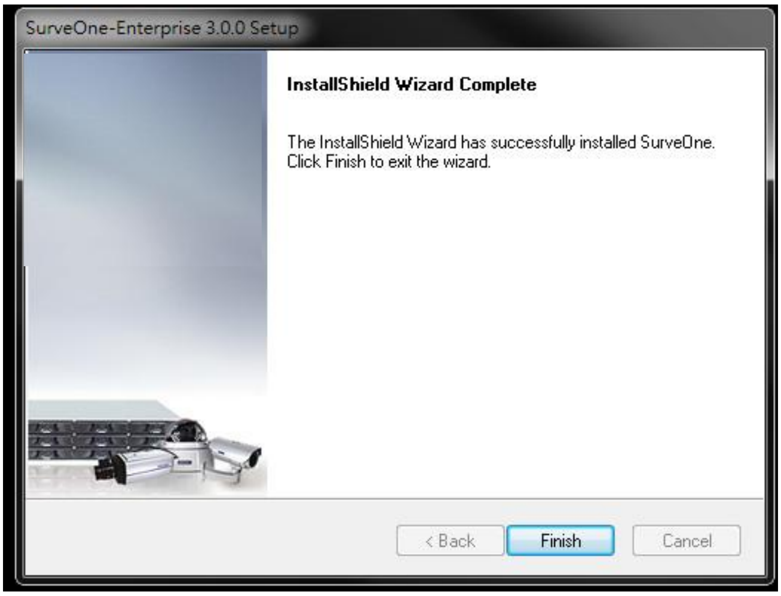
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

13. Once the installation is complete, click **Finish**.

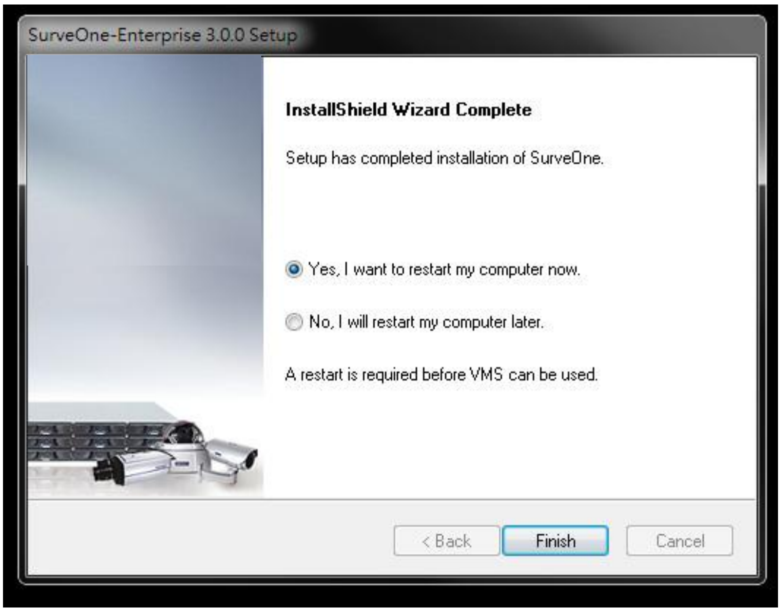


SurveOne-Enterprise 3.0.0 Setup

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed SurveOne. Click Finish to exit the wizard.

14. Restart your computer to activate the changes. Click **Finish** to exit.



SurveOne-Enterprise 3.0.0 Setup

InstallShield Wizard Complete

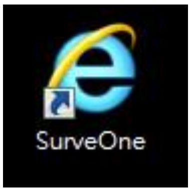
Setup has completed installation of SurveOne.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

A restart is required before VMS can be used.

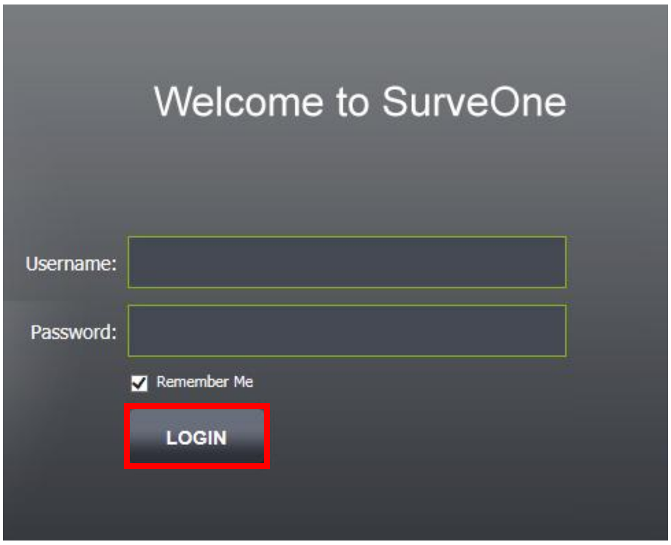
15. After the installation is done and your computer is restarted. On your desktop you’ll find an IE browser icon with SurveOne on it. Double click this icon to log in to the SurveOne and start monitor the overall system status.



13.2. Login

Log in to SurveOne:

1. Go to http://127.0.0.1:XX (XX is the port you have setup in the installation wizard.)
2. Input the default username and password, admin and admin.
3. Click **LOGIN**.



Welcome to SurveOne

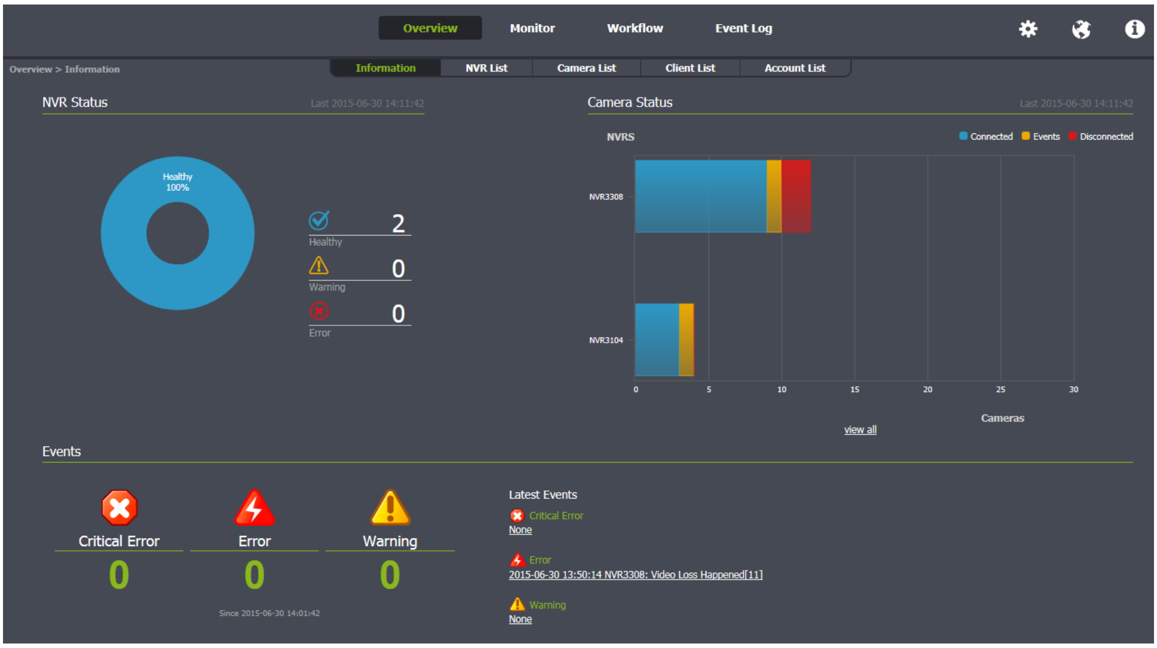
Username:

Password:

☑ Remember Me

13.3. Overview

Real-time System Status Information - The overall status of NVRs, cameras, and storage is displayed graphically, allowing users to grasp how the systems are at a glance.



Latest Events

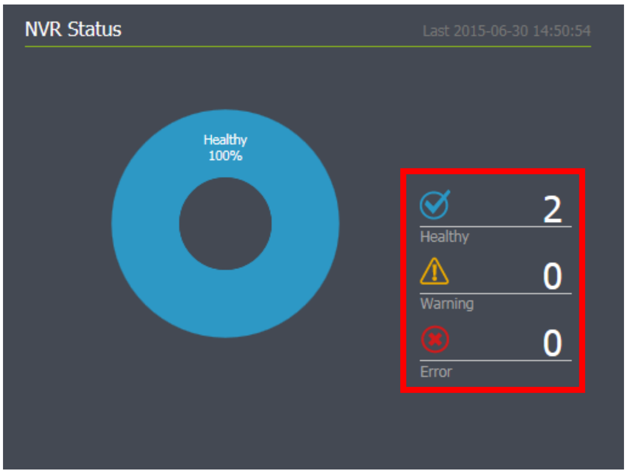
Critical Error
None

Error
2015-06-30 13:50:14 NVR3308: Video Loss Happened[11]

Warning
None

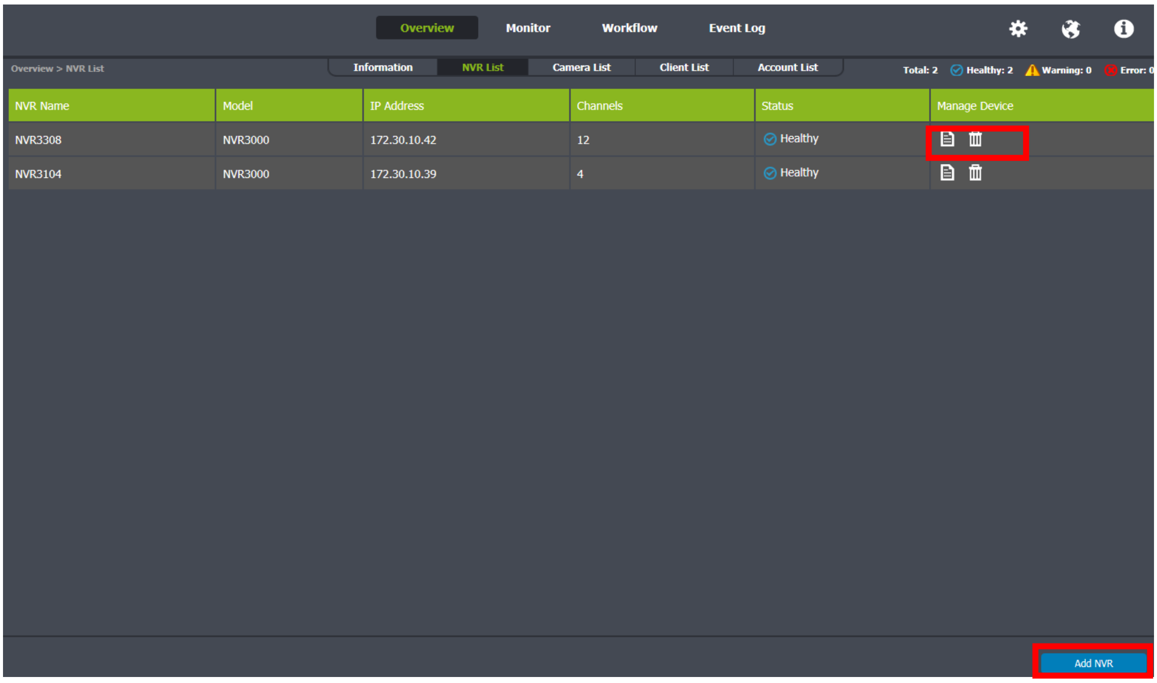
13.3.1. NVR Status

NVR status is classified into 3 groupings, Healthy, Warning and Error. Click on the status to see the details.



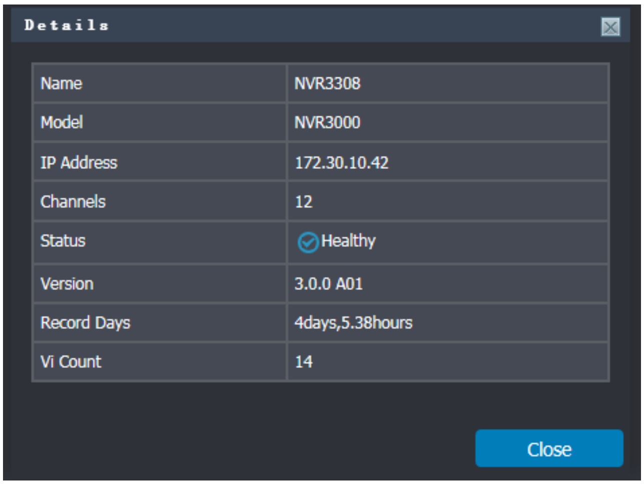
13.3.2. NVR List

After clicking on the status, the system will take you to the NVR List to see the detailed NVR status with information such as NVR name, model, IP address, channels and status.



NVR Name	Model	IP Address	Channels	Status	Manage Device
NVR3308	NVR3000	172.30.10.42	12	✓ Healthy	🗎 🗑
NVR3104	NVR3000	172.30.10.39	4	✓ Healthy	🗎 🗑

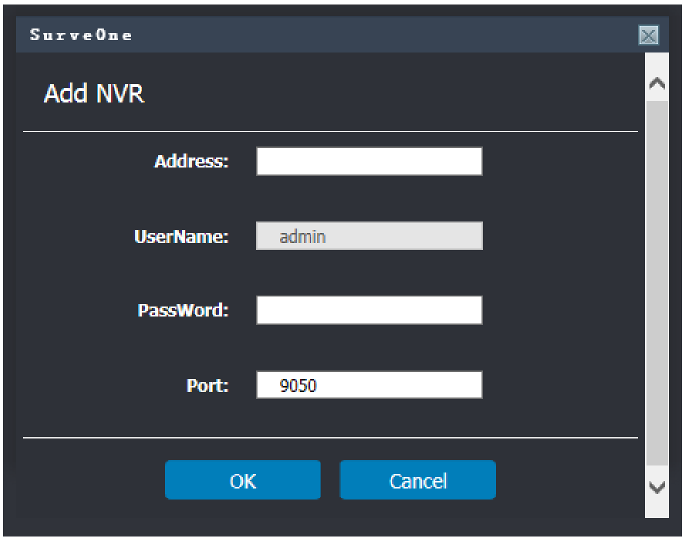
Click on the 🗎 to see the details of the NVR, including name, model, IP address, channels, status, version, record days, and VI counts.



Name	NVR3308
Model	NVR3000
IP Address	172.30.10.42
Channels	12
Status	✓ Healthy
Version	3.0.0 A01
Record Days	4days,5.38hours
Vi Count	14

Click on the 🗑 to remove the NVR.

Click Add NVR and fill out the pop-up form to add NVR.



SurveOne

Add NVR

Address:

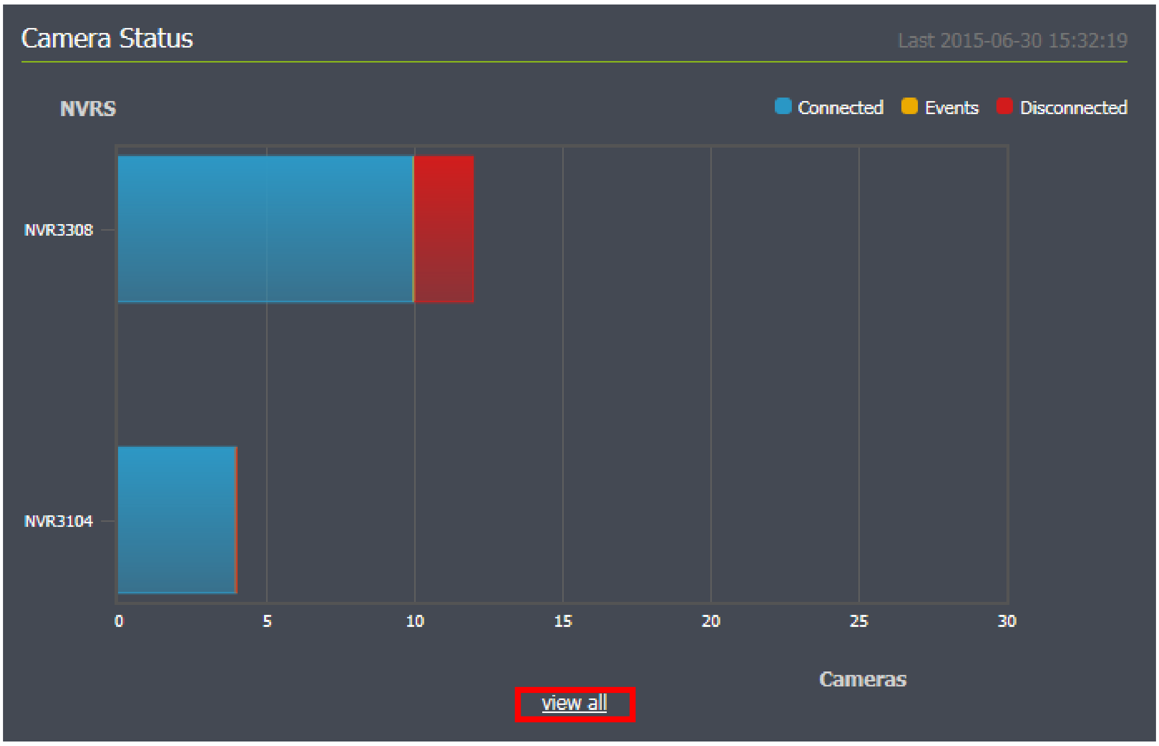
UserName: admin

PassWord:

Port: 9050

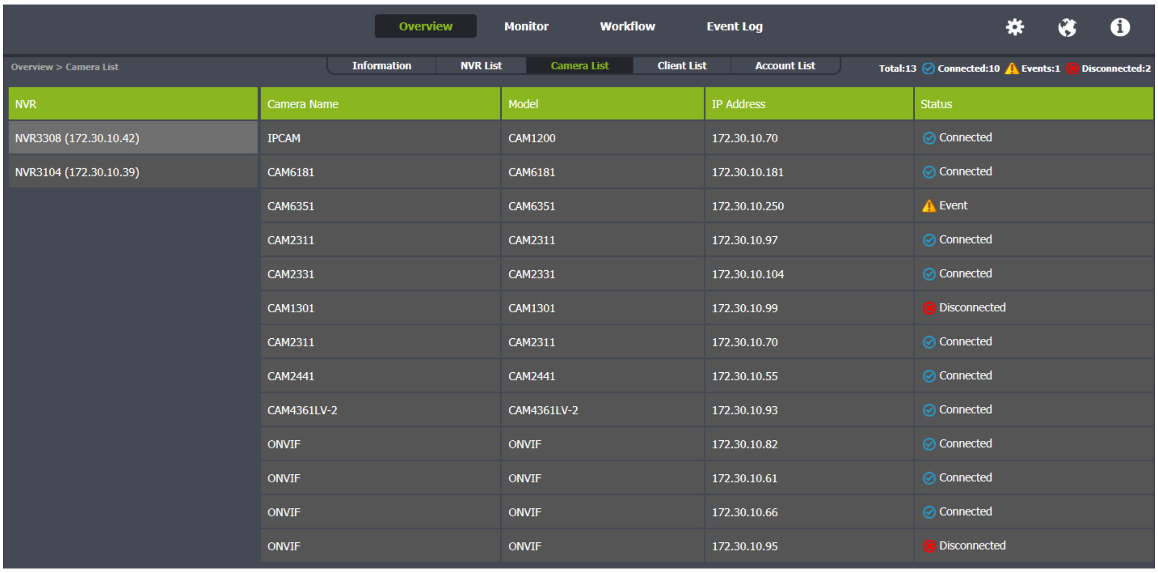
13.3.3. Camera Status

Camera status is classified into 3 groupings, Connected, Events, and Disconnected. Click on the view all to see the details.



13.3.4. Camera List

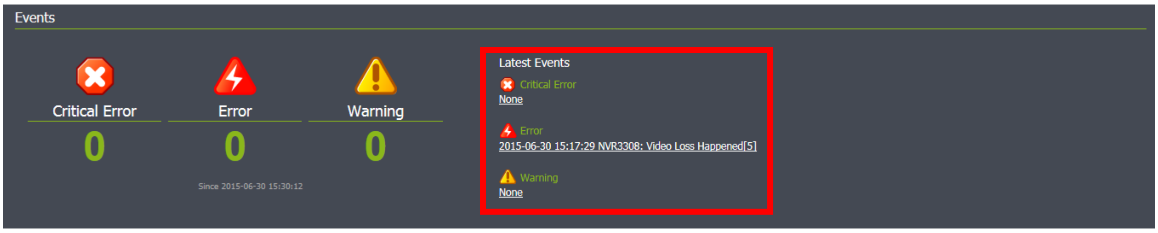
After clicking on the view all, the system will take you to the Camera List to see the detailed Camera status with information such as camera name, model, IP address, and status. Cameras under different NVR will be listed separately.



NVR	Camera Name	Model	IP Address	Status
NVR3308 (172.30.10.42)	IPCAM	CAM1200	172.30.10.70	✓ Connected
NVR3104 (172.30.10.39)	CAM6181	CAM6181	172.30.10.181	✓ Connected
	CAM6351	CAM6351	172.30.10.250	⚠ Event
	CAM2311	CAM2311	172.30.10.97	✓ Connected
	CAM2331	CAM2331	172.30.10.104	✓ Connected
	CAM1301	CAM1301	172.30.10.99	✗ Disconnected
	CAM2311	CAM2311	172.30.10.70	✓ Connected
	CAM2441	CAM2441	172.30.10.55	✓ Connected
	CAM4361LV-2	CAM4361LV-2	172.30.10.93	✓ Connected
	ONVIF	ONVIF	172.30.10.82	✓ Connected
	ONVIF	ONVIF	172.30.10.61	✓ Connected
	ONVIF	ONVIF	172.30.10.66	✓ Connected
	ONVIF	ONVIF	172.30.10.95	✗ Disconnected

13.3.5. Events Status

NVR and camera event logs are presented in real-time and classified into 3 groups: critical error, error, and warning, for easy management.



Latest Events

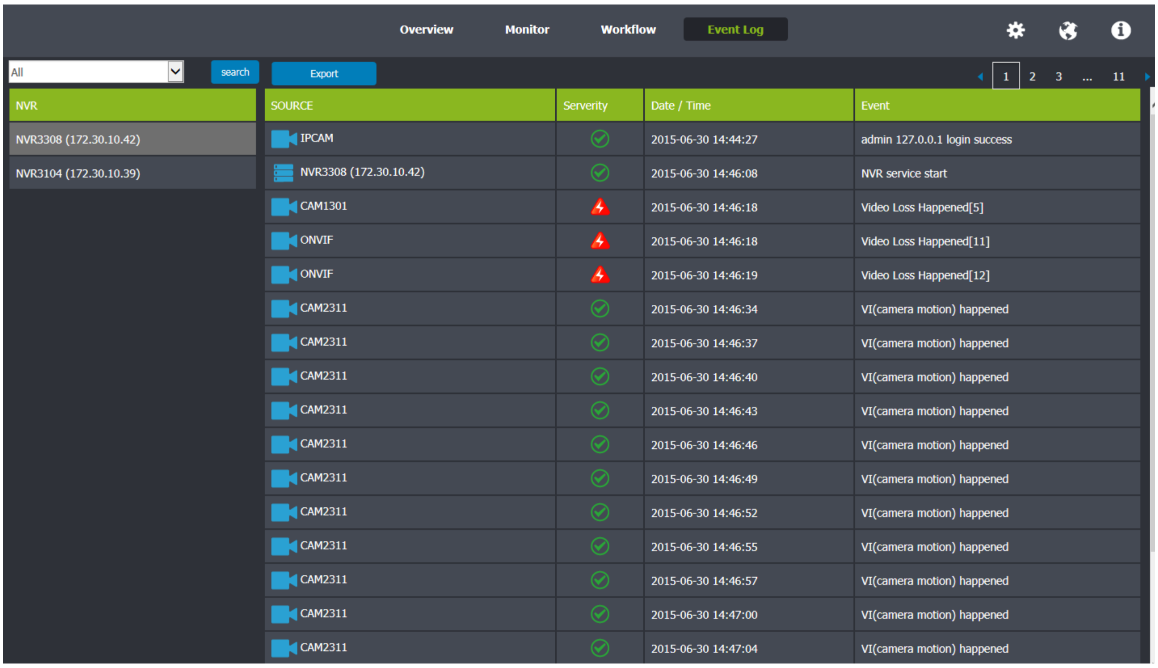
Critical Error
None

Error
2015-06-30 15:17:29 NVR3308: Video Loss Happened[5]

Warning
None

13.3.6. Event Log

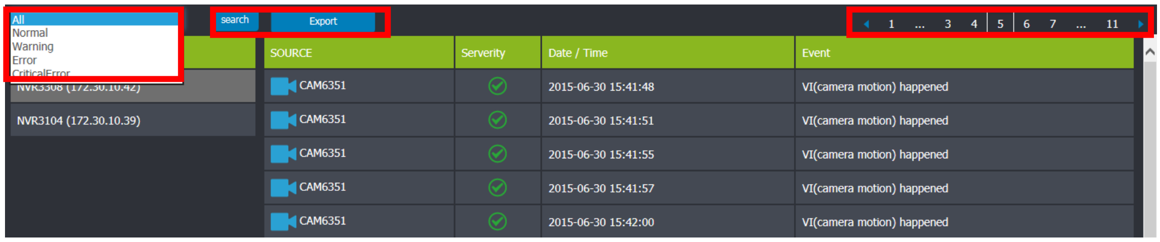
After clicking on the Latest Events, the system will take you to the Event Log to see the detailed event status with information such as source, severity, date/Time and Event. With classified event logs, users can identify which event needs to take actions first and which not to respond to the situations more quickly and efficiently.



NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

SOURCE	Serverity	Date / Time	Event
IPCAM	✓	2015-06-30 14:44:27	admin 127.0.0.1 login success
NVR3308 (172.30.10.42)	✓	2015-06-30 14:46:08	NVR service start
CAM1301	⚠	2015-06-30 14:46:18	Video Loss Happened[5]
ONVIF	⚠	2015-06-30 14:46:18	Video Loss Happened[11]
ONVIF	⚠	2015-06-30 14:46:19	Video Loss Happened[12]
CAM2311	✓	2015-06-30 14:46:34	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:37	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:40	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:43	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:46	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:49	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:52	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:55	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:57	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:47:00	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:47:04	VI(camera motion) happened

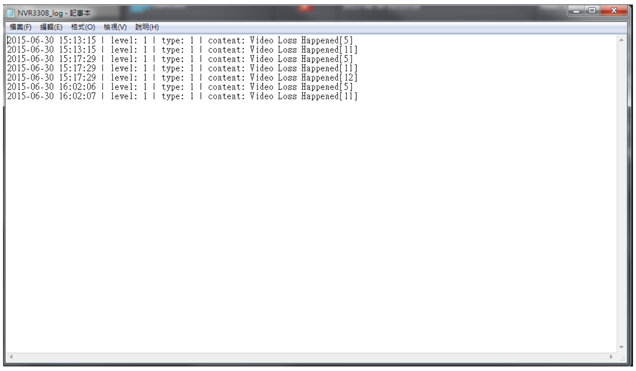
Use the drop-down list to filter the specific event, such as All, Normal, Warning, Error, Critical Error, you'd like to search and click Search or Export.



NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

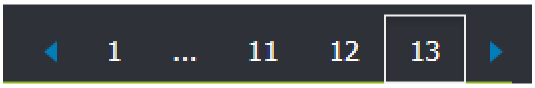
SOURCE	Serverity	Date / Time	Event
CAM6351	✓	2015-06-30 15:41:48	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:41:51	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:41:55	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:41:57	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:42:00	VI(camera motion) happened

Click Export, the log you're looking for will be copied to the notebook as shown below.



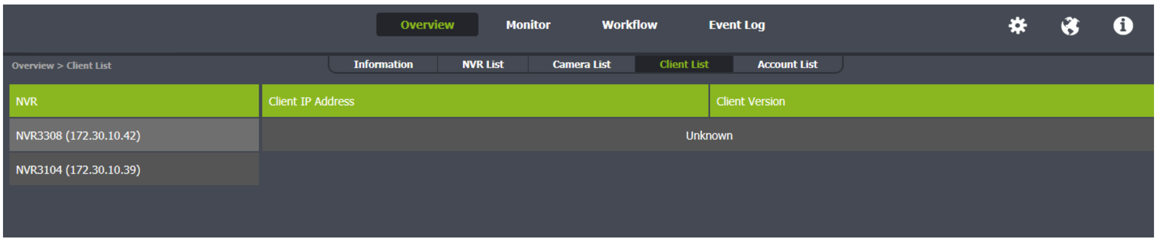
```
2015-06-30 15:13:15 | level: 1 | type: 1 | content: Video Loss Happened[5]
2015-06-30 15:13:15 | level: 1 | type: 1 | content: Video Loss Happened[11]
2015-06-30 15:17:29 | level: 1 | type: 1 | content: Video Loss Happened[5]
2015-06-30 15:17:29 | level: 1 | type: 1 | content: Video Loss Happened[11]
2015-06-30 15:17:29 | level: 1 | type: 1 | content: Video Loss Happened[12]
2015-06-30 16:02:06 | level: 1 | type: 1 | content: Video Loss Happened[5]
2015-06-30 16:02:07 | level: 1 | type: 1 | content: Video Loss Happened[11]
```

Click on the number on the upper right corner to jump to the corresponding page to see the log.



13.3.7. Client List

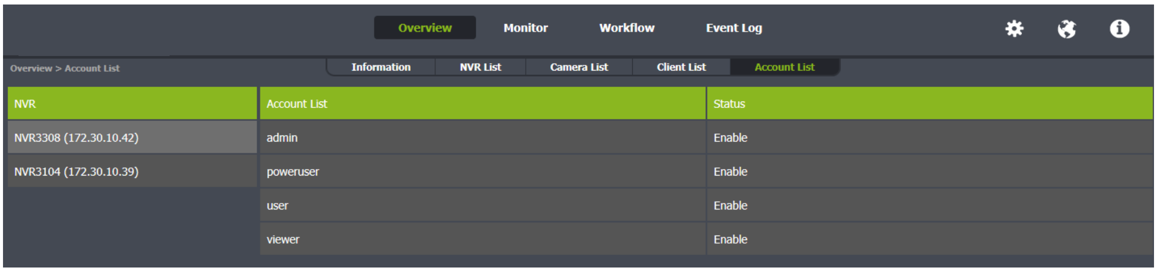
See the client information such as the client IP address and the client version here.



NVR	Client IP Address	Client Version
NVR3308 (172.30.10.42)	Unknown	
NVR3104 (172.30.10.39)		

13.3.8. Account List

See the account information such as the account list and the status here.



NVR	Account List	Status
NVR3308 (172.30.10.42)	admin	Enable
NVR3104 (172.30.10.39)	poweruser	Enable
	user	Enable
	viewer	Enable

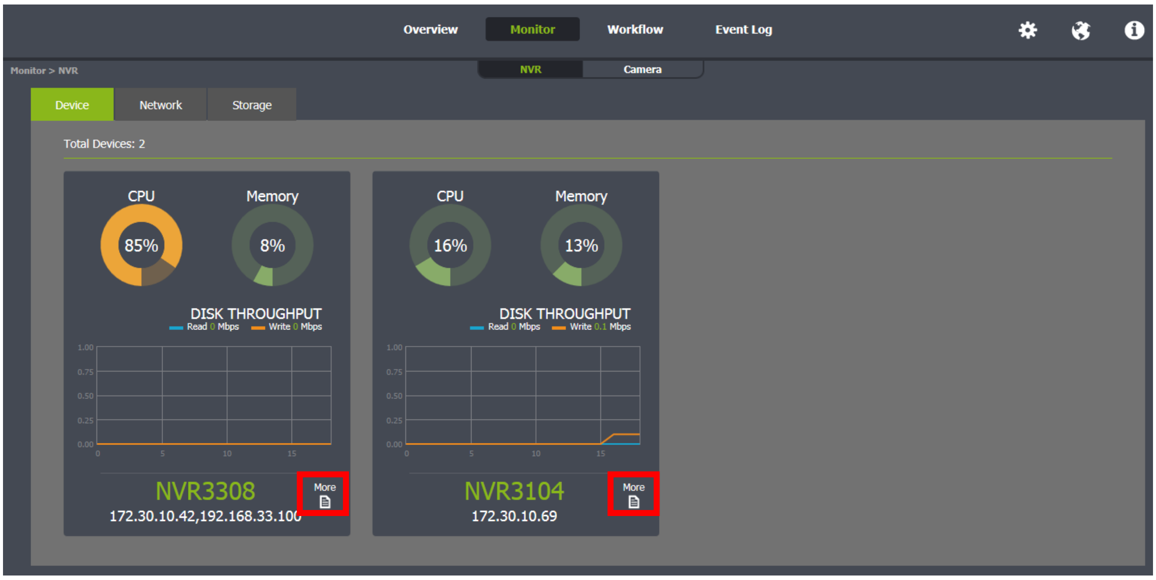
13.4. Monitor

As long as there is network connectivity, users can easily monitor the system status locally or remotely and ensure the consistent stability.

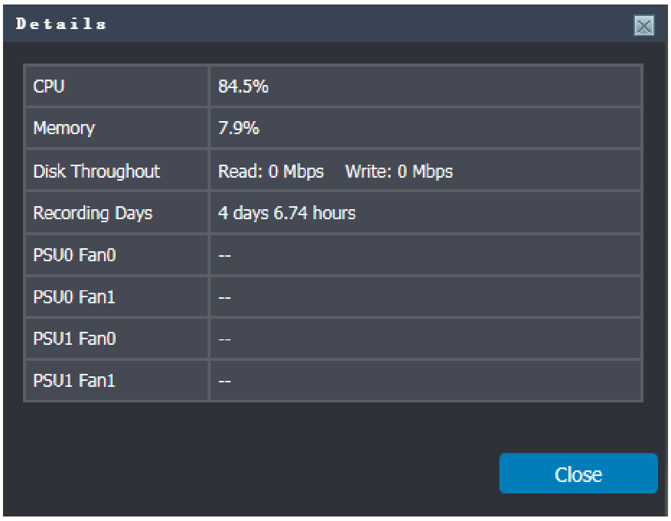
13.4.1. NVR

Device

See the connected NVR information including CPU, memory, and disk throughput graphically.



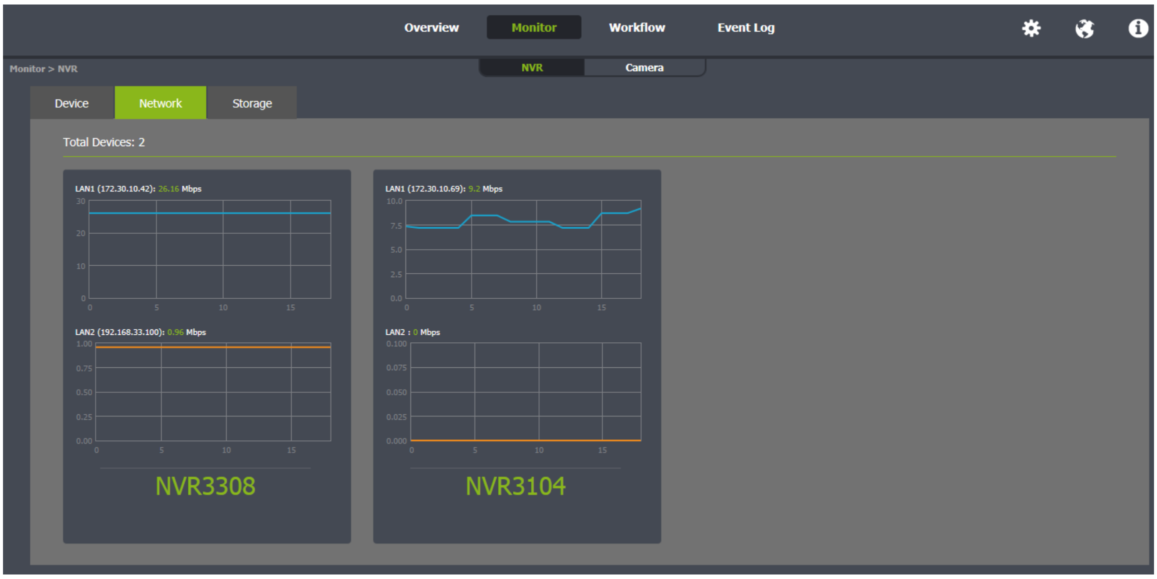
Click on the More to bring out the following chart to learn the details.



CPU	84.5%
Memory	7.9%
Disk Throughout	Read: 0 Mbps Write: 0 Mbps
Recording Days	4 days 6.74 hours
PSU0 Fan0	--
PSU0 Fan1	--
PSU1 Fan0	--
PSU1 Fan1	--

Network

See the network status graphically.



Total Devices: 2

LAN1 (172.30.10.42): 26.16 Mbps

LAN2 (192.168.33.100): 0.96 Mbps

NVR3308

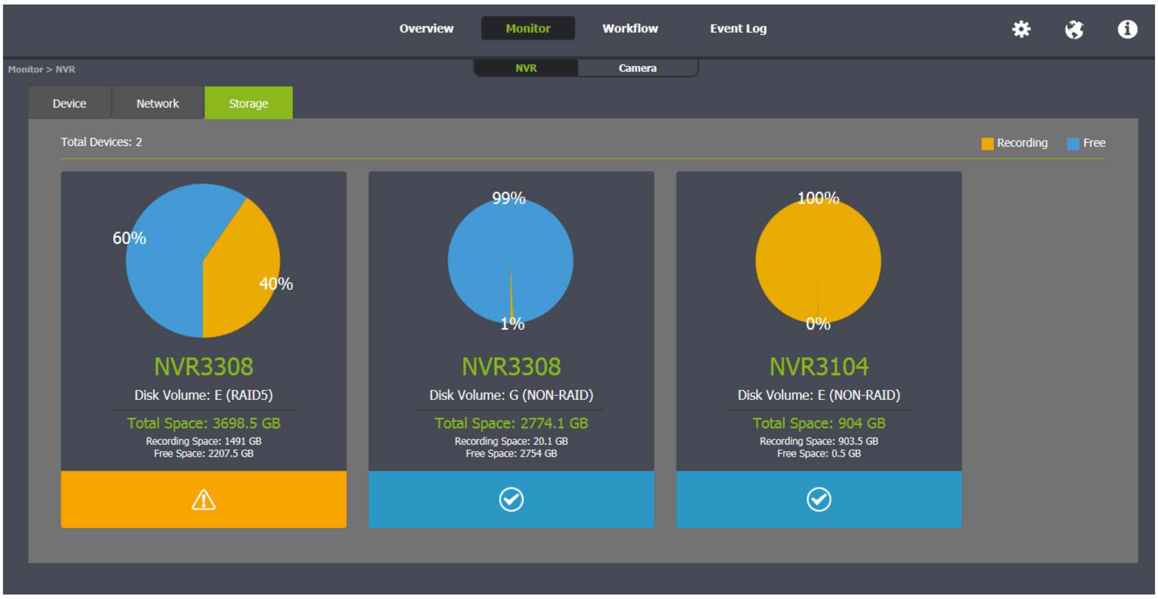
LAN1 (172.30.10.69): 9.2 Mbps

LAN2 : 0 Mbps

NVR3104

Storage

See the storage status including disk volume, space information graphically.



Total Devices: 2

NVR3308

Disk Volume: E (RAID5)

Total Space: 3698.5 GB

Recording Space: 1491 GB

Free Space: 2207.5 GB

NVR3308

Disk Volume: G (NON-RAID)

Total Space: 2774.1 GB

Recording Space: 20.1 GB

Free Space: 2754 GB

NVR3104

Disk Volume: E (NON-RAID)

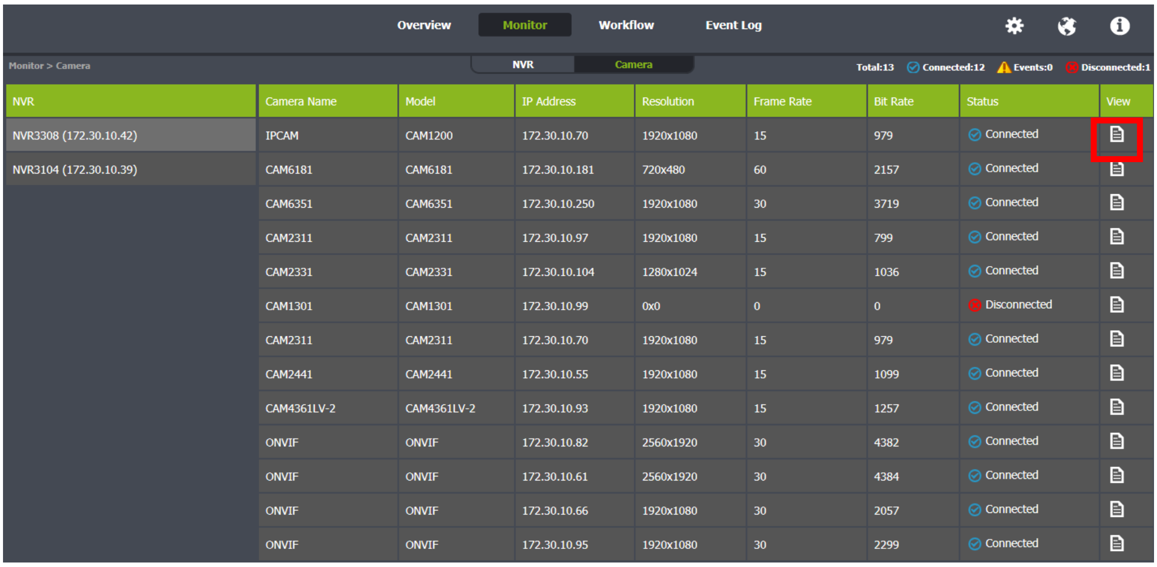
Total Space: 904 GB

Recording Space: 903.5 GB

Free Space: 0.5 GB

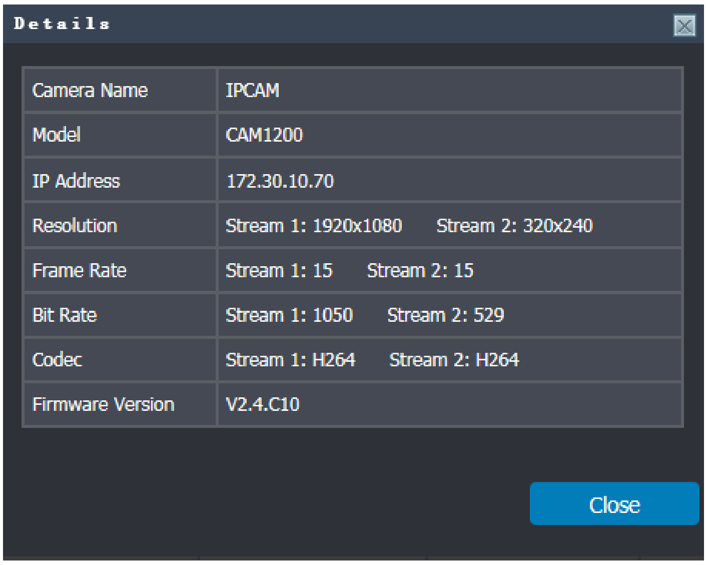
13.4.2. Camera

See the connected camera information including camera name, model, IP address, resolution, frame rate, bit rate, and status here.



NVR	Camera Name	Model	IP Address	Resolution	Frame Rate	Bit Rate	Status	View
NVR3308 (172.30.10.42)	IPCAM	CAM1200	172.30.10.70	1920x1080	15	979	Connected	🗎
NVR3104 (172.30.10.39)	CAM6181	CAM6181	172.30.10.181	720x480	60	2157	Connected	🗎
	CAM6351	CAM6351	172.30.10.250	1920x1080	30	3719	Connected	🗎
	CAM2311	CAM2311	172.30.10.97	1920x1080	15	799	Connected	🗎
	CAM2331	CAM2331	172.30.10.104	1280x1024	15	1036	Connected	🗎
	CAM1301	CAM1301	172.30.10.99	0x0	0	0	Disconnected	🗎
	CAM2311	CAM2311	172.30.10.70	1920x1080	15	979	Connected	🗎
	CAM2441	CAM2441	172.30.10.55	1920x1080	15	1099	Connected	🗎
	CAM4361LV-2	CAM4361LV-2	172.30.10.93	1920x1080	15	1257	Connected	🗎
	ONVIF	ONVIF	172.30.10.82	2560x1920	30	4382	Connected	🗎
	ONVIF	ONVIF	172.30.10.61	2560x1920	30	4384	Connected	🗎
	ONVIF	ONVIF	172.30.10.66	1920x1080	30	2057	Connected	🗎
	ONVIF	ONVIF	172.30.10.95	1920x1080	30	2299	Connected	🗎

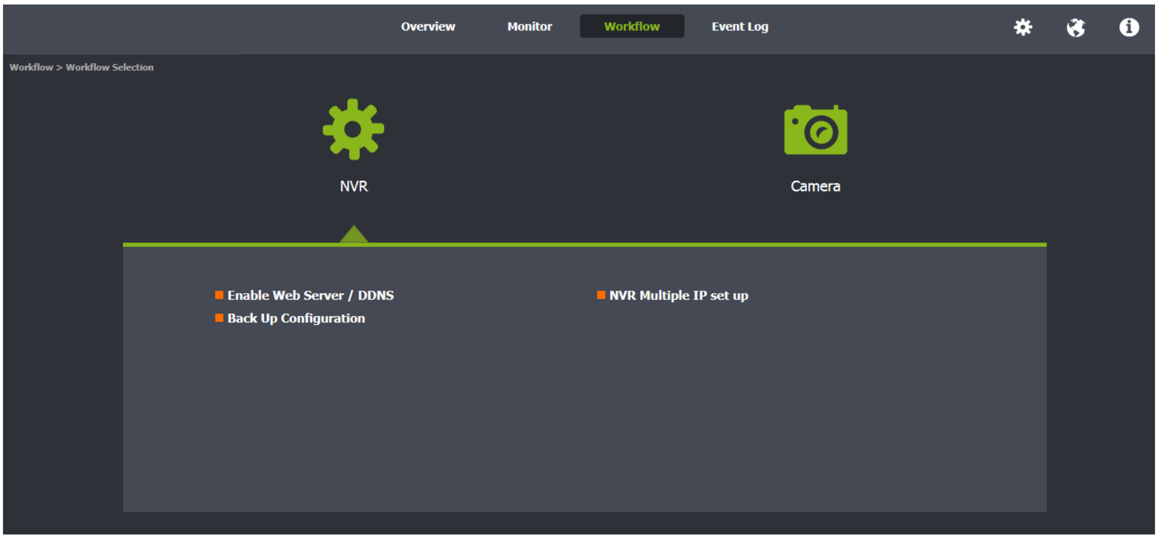
Click on the 🗎 to see more details, such as camera name, model, IP address, resolution, frame rate, bit rate, codec, and firmware version.



Camera Name	IPCAM
Model	CAM1200
IP Address	172.30.10.70
Resolution	Stream 1: 1920x1080 Stream 2: 320x240
Frame Rate	Stream 1: 15 Stream 2: 15
Bit Rate	Stream 1: 1050 Stream 2: 529
Codec	Stream 1: H264 Stream 2: H264
Firmware Version	V2.4.C10

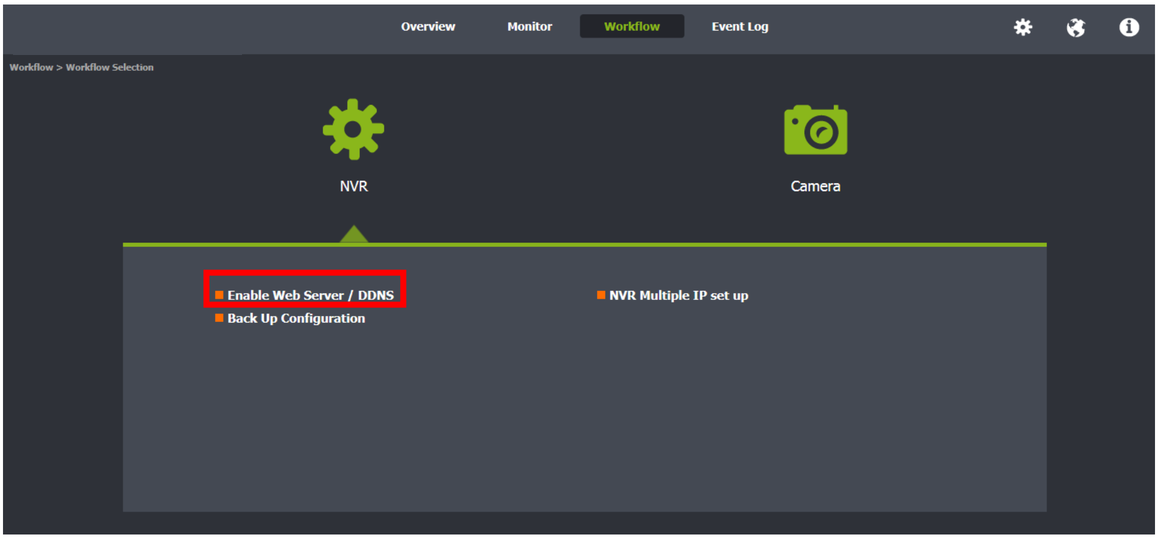
13.5. Workflow

Designed for easy configuration, deployment and maintenance, SurveOne allows users to do one-time setup. Users can simply copy the NVR or camera configurations and apply them to new devices to ease the complicated setup process. The configurations can also be saved as backup and restored when needed.



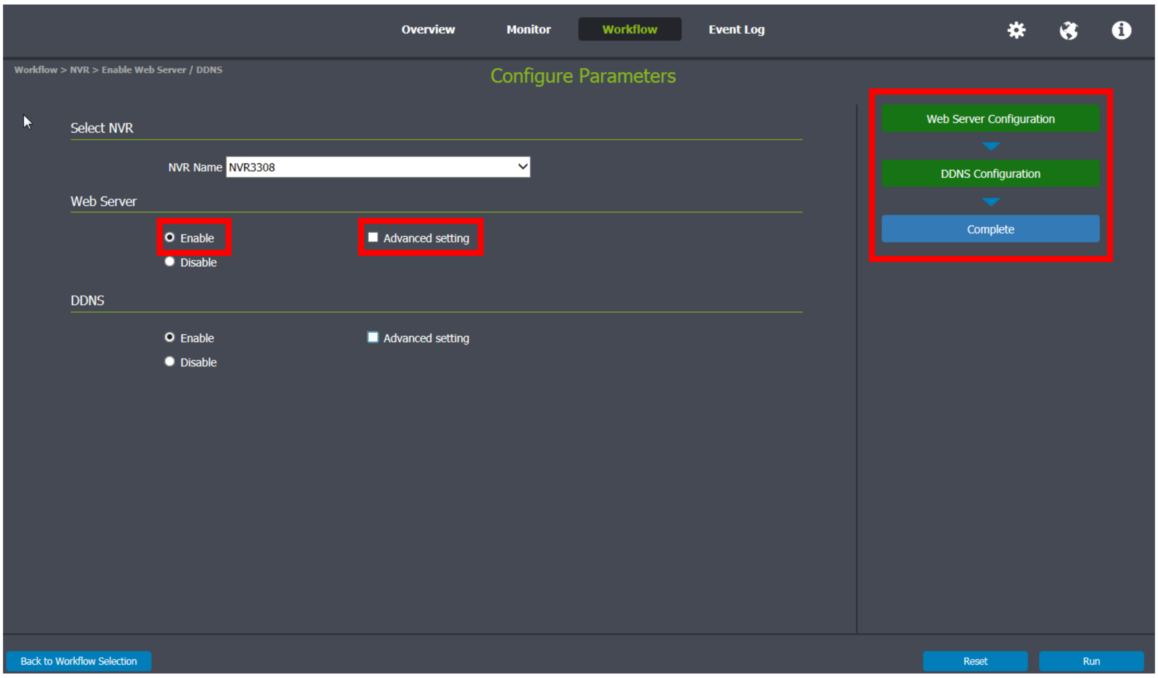
13.5.1. NVR

Enable Web Server / DDNS



Web Server

Follow the instruction flow on the right. Users can set up the Web server/DDNS here. Click **Enable** to activate the functionalities. You can also click **Advanced Setting** to fill in further information.



Configure Parameters

Select NVR

NVR Name: NVR3308

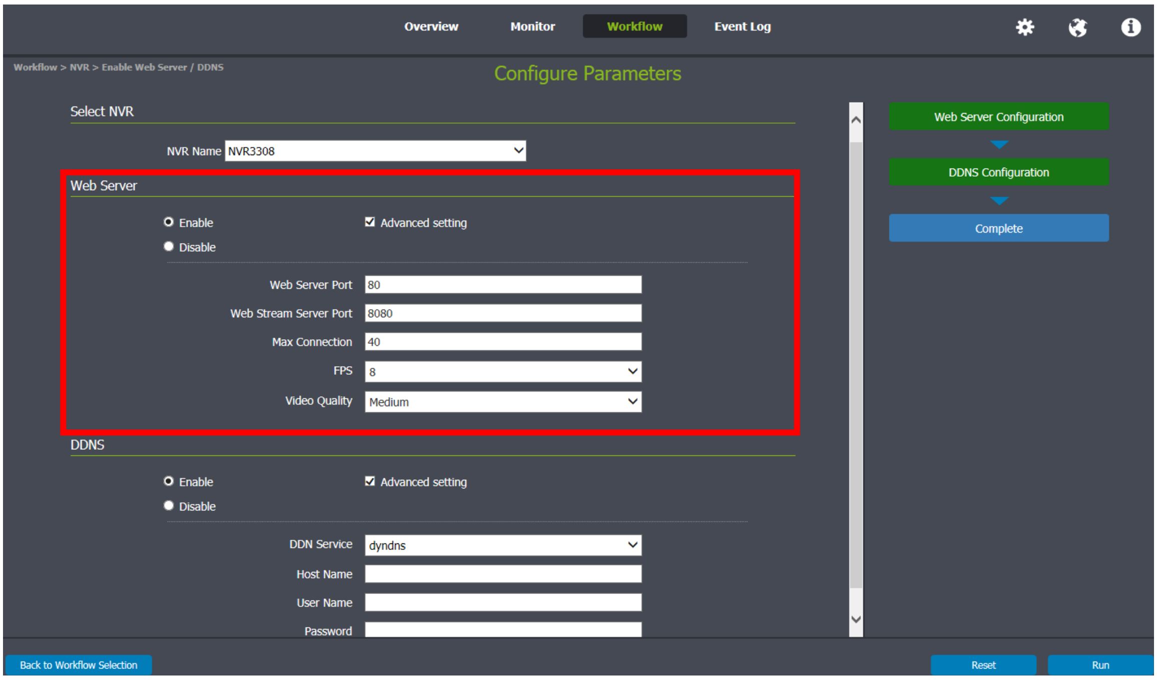
Web Server

○ Enable ☐ Advanced setting
● Disable

DDNS

○ Enable ☐ Advanced setting
● Disable

Enable the Web Server and click **Advanced setting** to fill in the following information for the Web Server settings to use the Web Client/Mobile Client.



Configure Parameters

Select NVR

NVR Name: NVR3308

Web Server

○ Enable ☑ Advanced setting
● Disable

Web Server Port: 80
Web Stream Server Port: 8080
Max Connection: 40
FPS: 8
Video Quality: Medium

DDNS

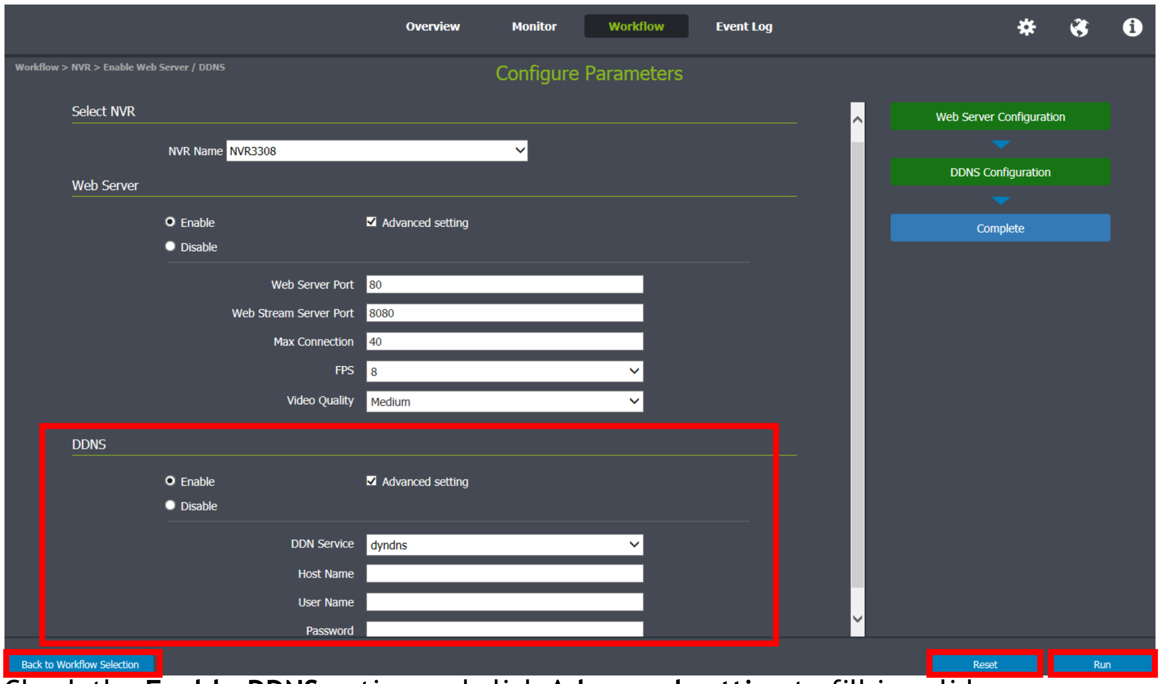
○ Enable ☑ Advanced setting
● Disable

DDN Service: dyndns
Host Name:
User Name:
Password:

Note: (1) User may just keep the default settings in the Web Server. (2) Do not set the Web Server Port as these port numbers – 8080 (Web Stream Port), 9090 (NVR Stream Port), 2809 (NVR Server Login Port), 7735 (TV Wall Port (2.5.0)), 7734, 1024, 9010 (Domain Broadcast Port), 9030 (Domain Client Message Port), 9040 (Domain Console Message Port), 9050 (Domain Local Communication Port), 9020 (Domain Remote Communication Port), 9080 (Domain Local Log Data Download Port), 9081 (Domain Remote Log Data Download Port), 9060 (Domain Local Data Port), 9061 (Domain Remote Data Port), 15507 (Domain Local Log Message Download Port), 15503 (Domain Remote Log Message Download Port), 15501 (Domain Remote Log Upload port), 15505 (Domain Local Log Upload Port), 40000 (NVR Broadcast Port), 50000 (NVR Message Port).

DDNS

DDNS (Dynamic Domain Name Server) is a protocol that enables the device to maintain a static connection address, even when its IP changes. Access using this feature is disabled by default. Connecting using DDNS requires registration on third-party websites for DDNS services.



Select NVR

NVR Name: NVR3308

Web Server

○ Enable ☑ Advanced setting
● Disable

Web Server Port: 80
Web Stream Server Port: 8080
Max Connection: 40
FPS: 8
Video Quality: Medium

DDNS

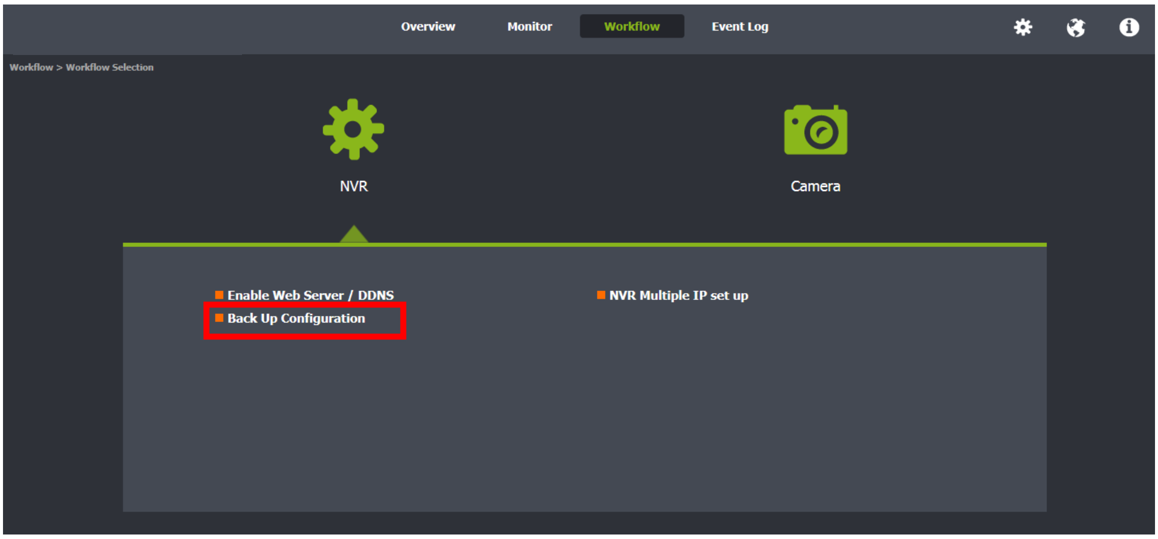
○ Enable ☑ Advanced setting
● Disable

DDN Service: dyndns
Host Name:
User Name:
Password:

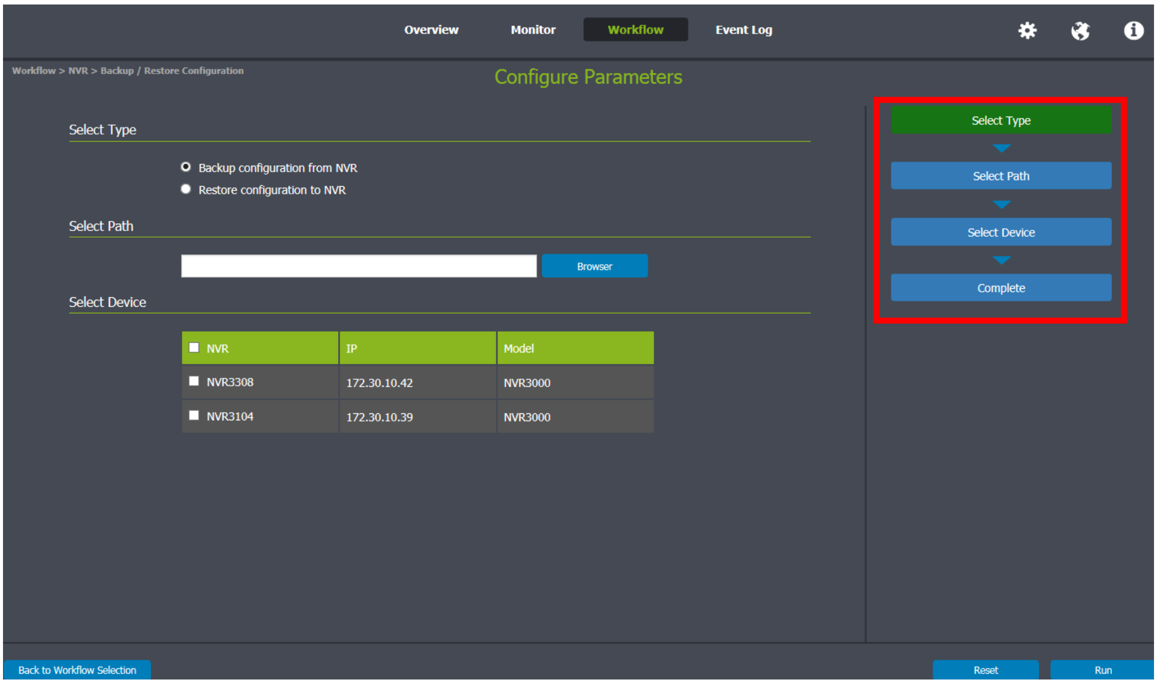
Check the **Enable DDNS** option and click **Advanced setting** to fill in valid user name and password. You can then access the device through the registered domain name.

- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

Back Up Configuration



Follow the instruction flow on the right. The configurations can be saved as backup and restored when needed to save time and effort.



Select Type

○ Backup configuration from NVR
○ Restore configuration to NVR

Select Path

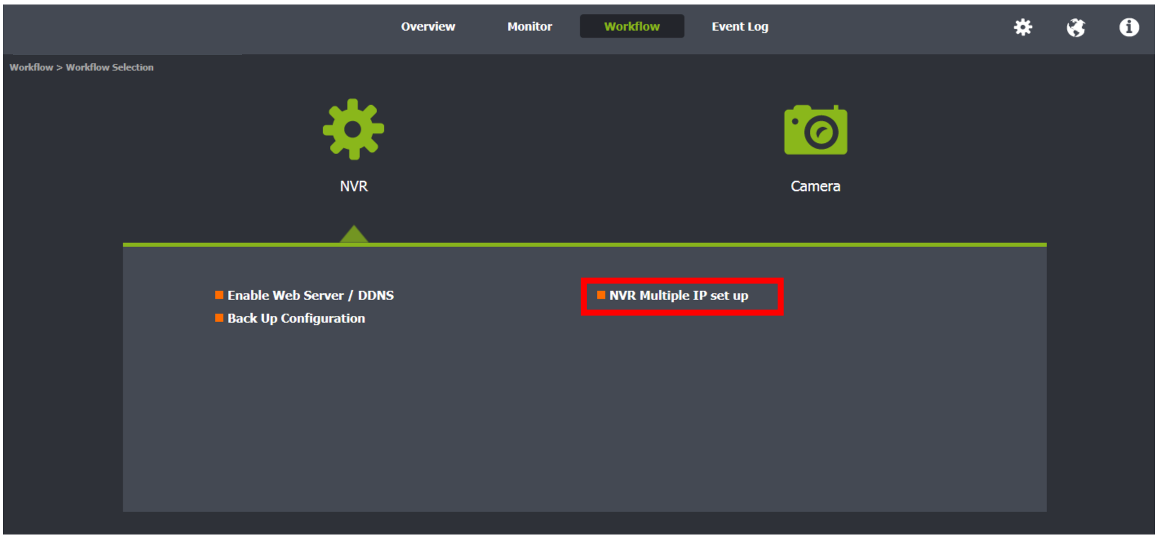
Select Device

□ NVR	IP	Model
□ NVR3308	172.30.10.42	NVR3000
□ NVR3104	172.30.10.39	NVR3000

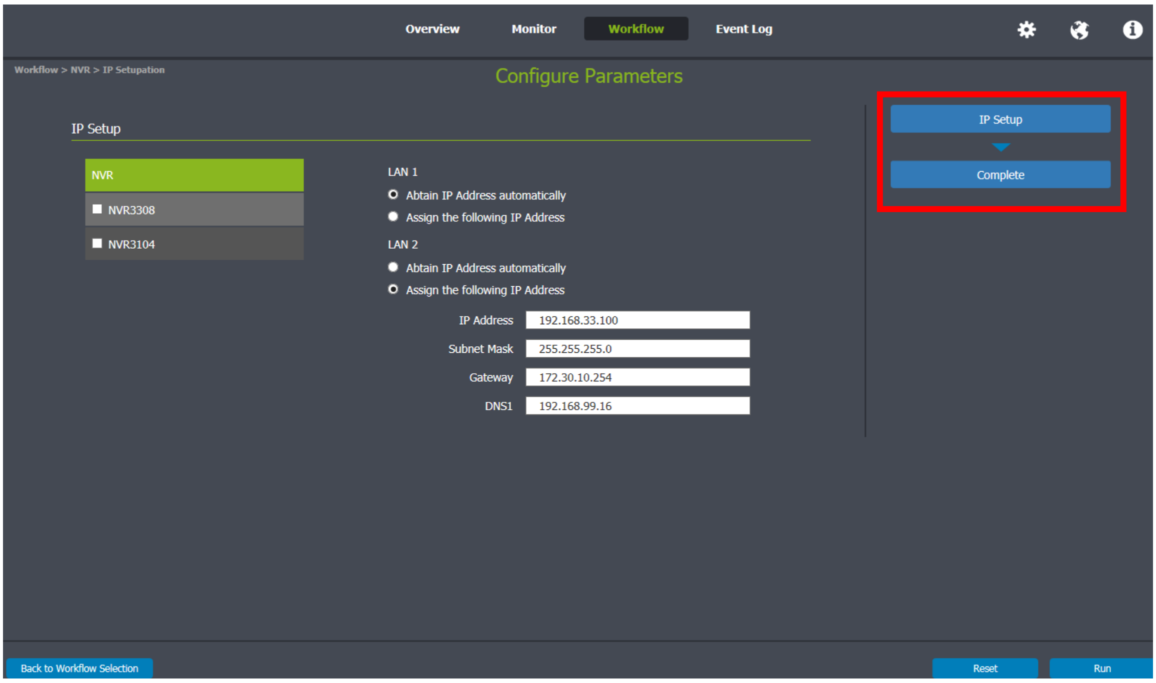
1. Select **Backup** or **Restore**.
2. Select path to save the configurations.
3. Select which device you'd like to save its configurations.

- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

NVR Multiple IP Setup



Follow the instruction flow on the right. Multiple IP addresses are supported. You can select the Obtain IP Address Automatically or Assign the following IP Address and input detailed information for each NVR.



IP Setup

NVR
- □ NVR3308
- □ NVR3104

LAN 1
- ○ Obtain IP Address automatically
- ● Assign the following IP Address

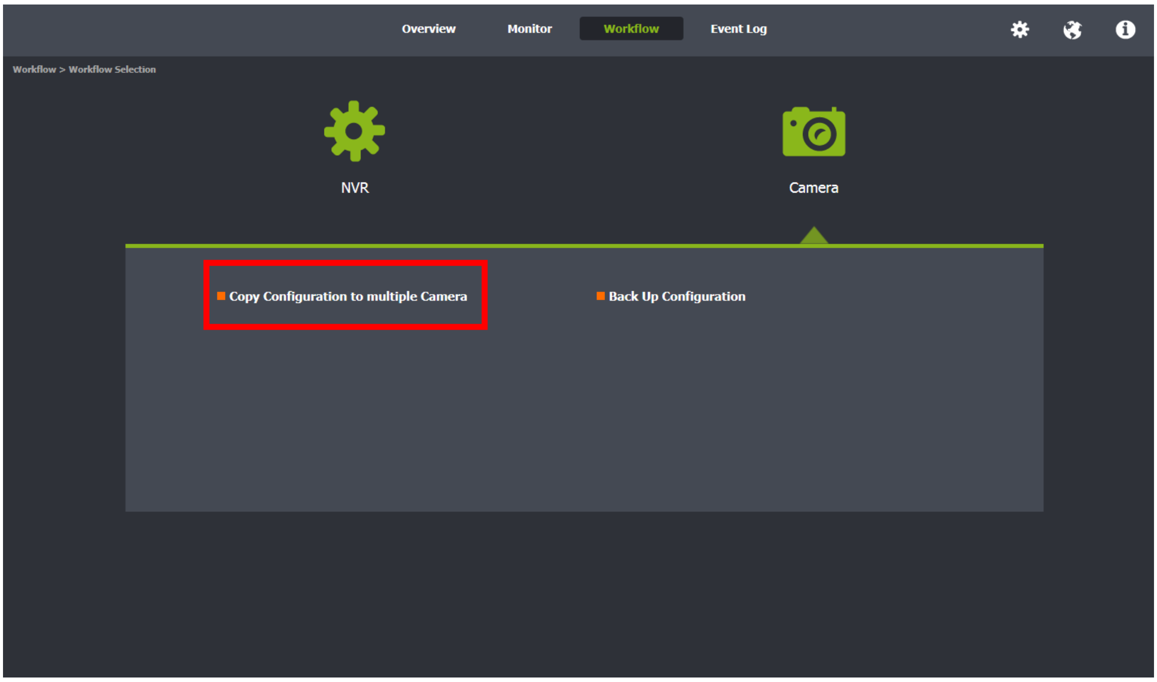
LAN 2
- ● Obtain IP Address automatically
- ○ Assign the following IP Address

IP Address	192.168.33.100
Subnet Mask	255.255.255.0
Gateway	172.30.10.254
DNS1	192.168.99.16

- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

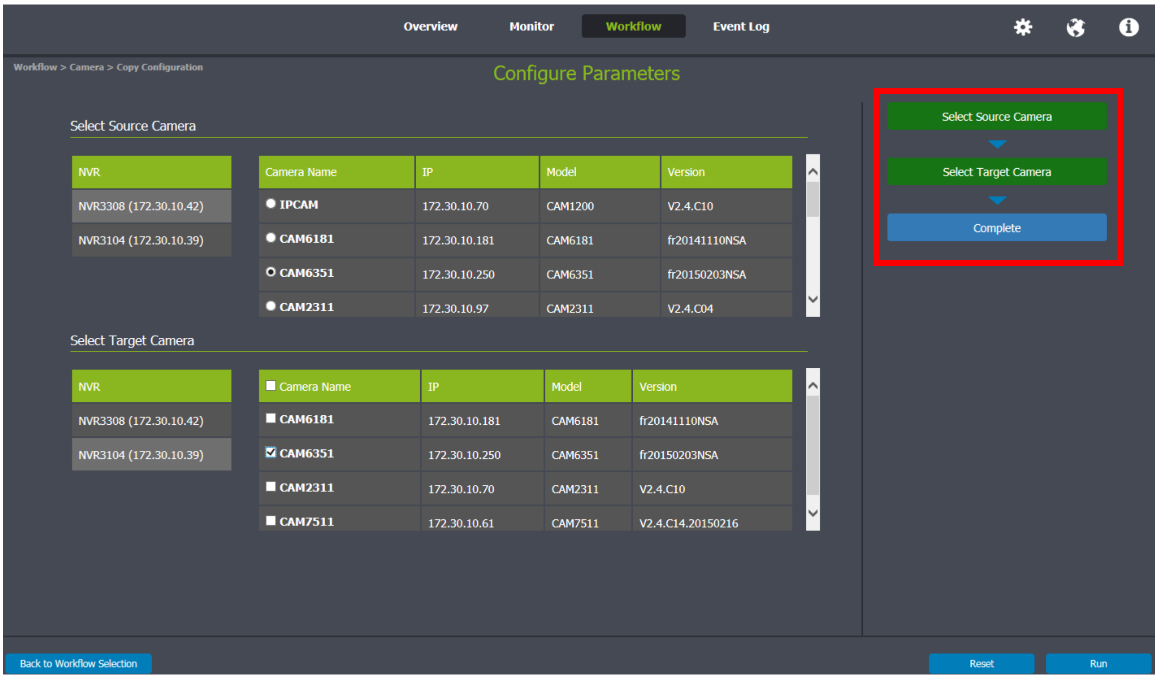
13.5.2. Camera

Copy Configuration to Multiple Cameras


Overview
Monitor
Workflow
Event Log
Workflow > Workflow Selection
NVR
Camera
Copy Configuration to multiple Camera
Back Up Configuration

Follow the instruction flow on the right. The configurations can be saved as backup and restored when needed to save time and effort.

> **Note:** The source camera and the target camera should bear the same model and version.



Select Source Camera

NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

Camera Name	IP	Model	Version
○ IPCAM	172.30.10.70	CAM1200	V2.4.C10
○ CAM6181	172.30.10.181	CAM6181	fr20141110NSA
● CAM6351	172.30.10.250	CAM6351	fr20150203NSA
○ CAM2311	172.30.10.97	CAM2311	V2.4.C04

Select Target Camera

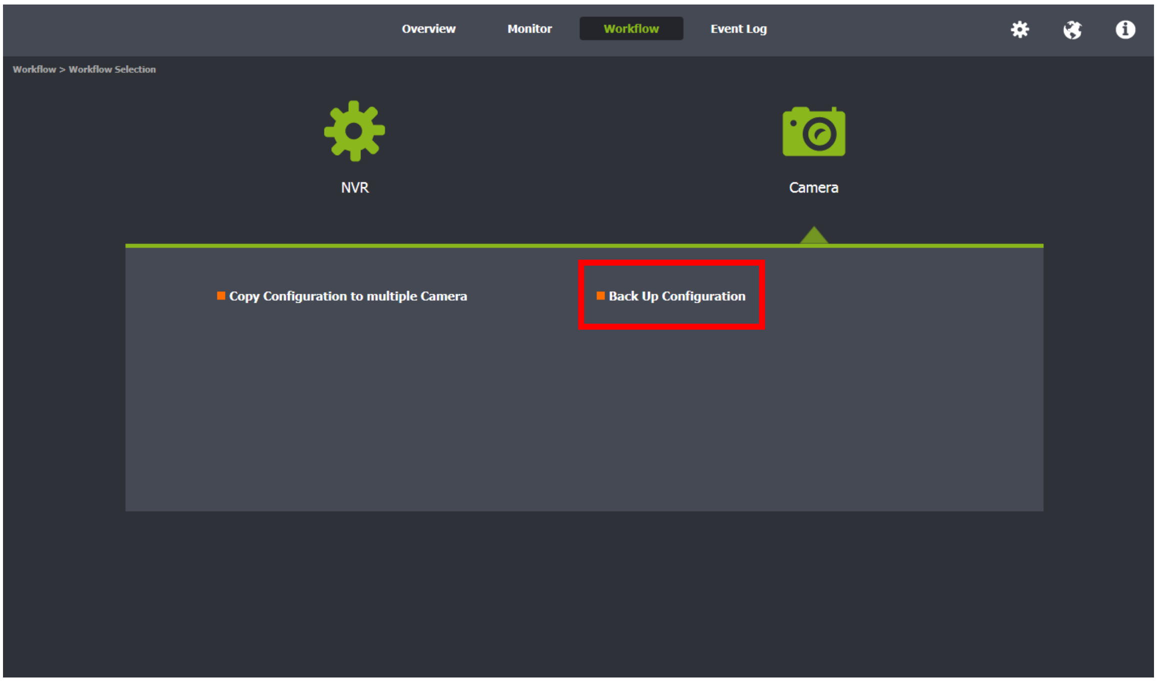
NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

□ Camera Name	IP	Model	Version
□ CAM6181	172.30.10.181	CAM6181	fr20141110NSA
☑ CAM6351	172.30.10.250	CAM6351	fr20150203NSA
□ CAM2311	172.30.10.70	CAM2311	V2.4.C10
□ CAM7511	172.30.10.61	CAM7511	V2.4.C14.20150216

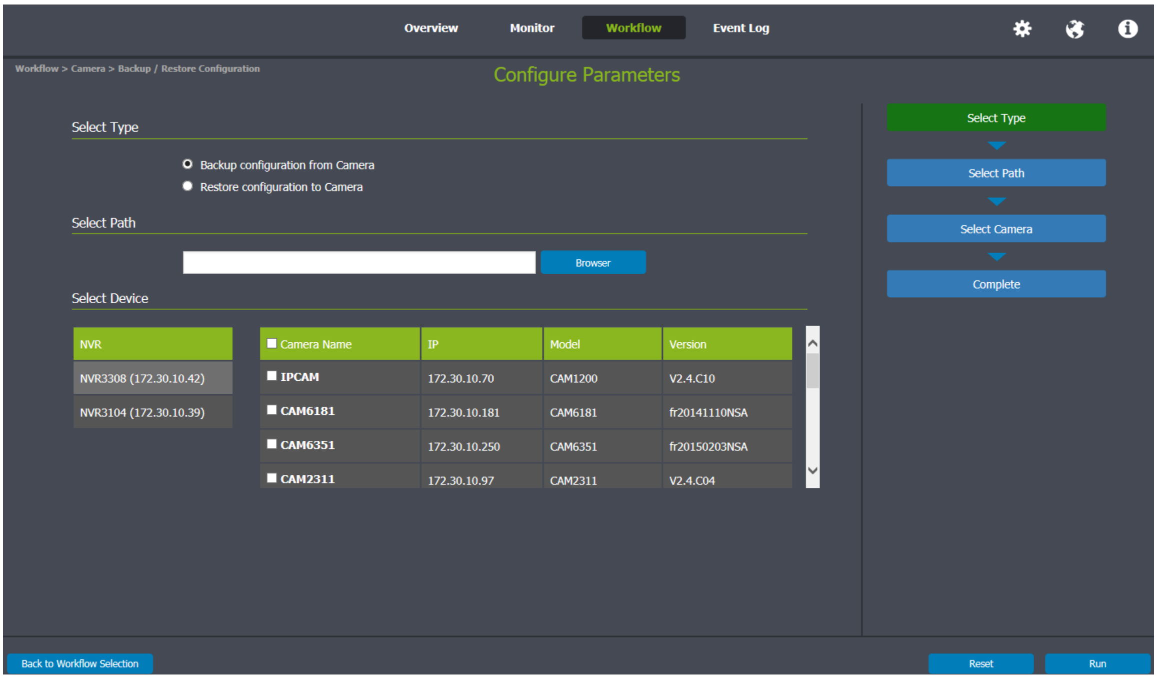
1. Select the source NVR and the cameras under this NVR.
2. Select the target NVR and the cameras under this NVR.

- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

Backup Configuration


Overview
Monitor
Workflow
Event Log
Workflow > Workflow Selection
NVR
Camera
Copy Configuration to multiple Camera
Back Up Configuration

Follow the instruction flow on the right. The configurations can be saved as backup and restored when needed to save time and effort.



Configure Parameters

Select Type

● Backup configuration from Camera
○ Restore configuration to Camera

Select Path

Select Device

NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

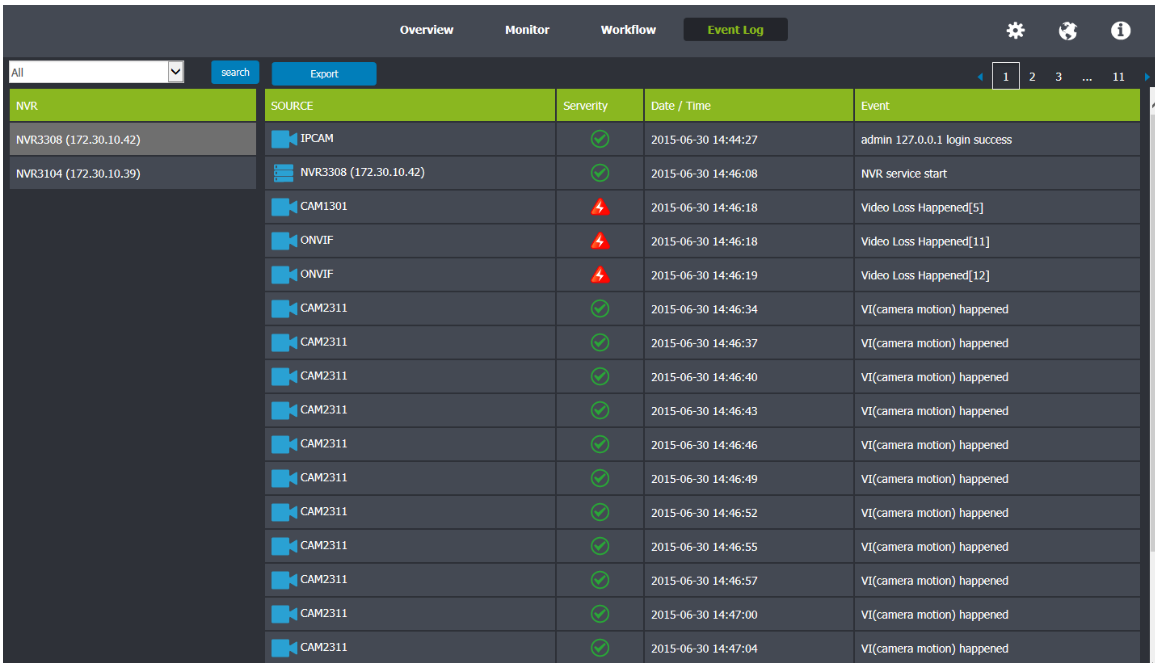
□ Camera Name	IP	Model	Version
□ IPCAM	172.30.10.70	CAM1200	V2.4.C10
□ CAM6181	172.30.10.181	CAM6181	fr20141110NSA
□ CAM6351	172.30.10.250	CAM6351	fr20150203NSA
□ CAM2311	172.30.10.97	CAM2311	V2.4.C04

1. Select **Backup** or **Restore**.
2. Select path to save the configurations.
3. Select which device you’d like to save its configurations.

- Click **Back to Workflow Selection** to go back to the previous setting page.
- Click **Reset** to reset settings on this page.
- Click **Run** to execute the setups now.

13.6. Event Log

See the detailed event status with information such as source, severity, date/Time and Event here. With classified event logs, users can identify which event needs to take actions first and which not to respond to the situations more quickly and efficiently.

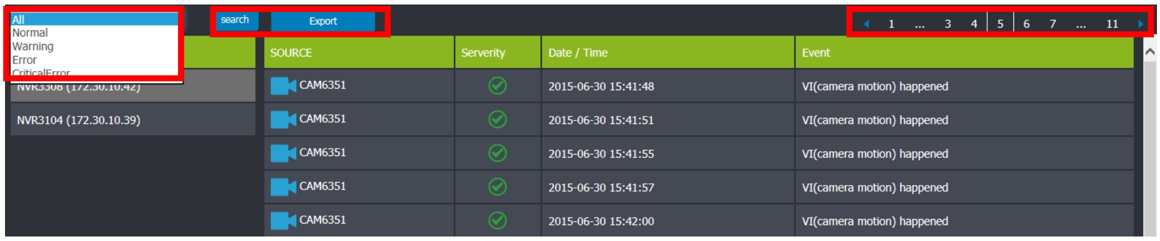


NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

SOURCE	Serverity	Date / Time	Event
IPCAM	✓	2015-06-30 14:44:27	admin 127.0.0.1 login success
NVR3308 (172.30.10.42)	✓	2015-06-30 14:46:08	NVR service start
CAM1301	⚠	2015-06-30 14:46:18	Video Loss Happened[5]
ONVIF	⚠	2015-06-30 14:46:18	Video Loss Happened[11]
ONVIF	⚠	2015-06-30 14:46:19	Video Loss Happened[12]
CAM2311	✓	2015-06-30 14:46:34	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:37	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:40	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:43	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:46	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:49	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:52	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:55	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:46:57	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:47:00	VI(camera motion) happened
CAM2311	✓	2015-06-30 14:47:04	VI(camera motion) happened

Search

Use the drop-down list to filter the specific event, such as All, Normal, Warning, Error, Critical Error, you'd like to search and click Search or Export.

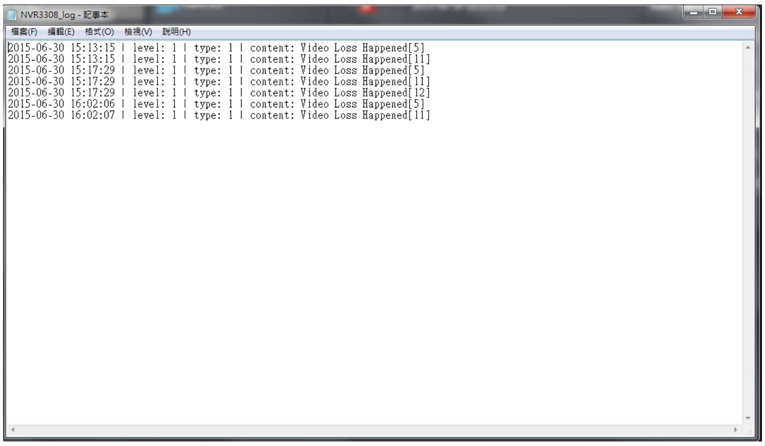


NVR
NVR3308 (172.30.10.42)
NVR3104 (172.30.10.39)

SOURCE	Serverity	Date / Time	Event
CAM6351	✓	2015-06-30 15:41:48	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:41:51	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:41:55	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:41:57	VI(camera motion) happened
CAM6351	✓	2015-06-30 15:42:00	VI(camera motion) happened

Export

Click Export, the log you’re looking for will be copied to the notebook as shown below.



```
2015-06-30 15:13:15 | level: 1 | type: 1 | content: Video Loss Happened[5]
2015-06-30 15:13:15 | level: 1 | type: 1 | content: Video Loss Happened[11]
2015-06-30 15:17:29 | level: 1 | type: 1 | content: Video Loss Happened[5]
2015-06-30 15:17:29 | level: 1 | type: 1 | content: Video Loss Happened[11]
2015-06-30 15:17:29 | level: 1 | type: 1 | content: Video Loss Happened[12]
2015-06-30 16:02:06 | level: 1 | type: 1 | content: Video Loss Happened[5]
2015-06-30 16:02:07 | level: 1 | type: 1 | content: Video Loss Happened[11]
```

Click on the number on the upper right corner to jump to the corresponding page to see the log.